MyPower VoIP Gateway Web Config Manual

V4.1

Maipu Communication Technology Co., Ltd
No. 16, JiuXing Avenue
Hi-Tech Park
Chengdu, Sichuan Province
P. R. China
610041
Tel: (86) 28-85148850, 85148041
Fax: (86) 28-85148948, 85148139
URL: http:// www.maipu.com
Mail: overseas@maipu.com

All rights reserved. Printed in the People's Republic of China.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without the prior written consent of Maipu Communication Technology Co., Ltd.

Maipu makes no representations or warranties with respect to this document contents and specifically disclaims any implied warranties of merchantability or fitness for any specific purpose. Further, Maipu reserves the right to revise this document and to make changes from time to time in its content without being obligated to notify any person of such revisions or changes.

Maipu values and appreciates comments you may have concerning our products or this document. Please address comments to:

Maipu Communication Technology Co., Ltd
No. 16, JiuXing Avenue, Hi-Tech Park
Chengdu, Sichuan Province
P. R. China
610041
Tel: (86) 28-85148850, 85148041
Fax: (86) 28-85148948, 85148139
URL: http:// www.maipu.com
Mail: overseas@maipu.com

All other products or services mentioned herein may be registered trademarks, trademarks, or service marks of their respective manufacturers, companies, or organizations.

Maipu Feedback Form

Your opinion helps us improve the quality of our product documentation and offer better services. Please fax your comments and suggestions to (86) 28-85148948, 85148139 or email to overseas@maipu.com.

<table>
<tr><td>Document Title</td><td colspan="4">MyPower VoIP Gateway WEB Config Manual V4.1</td></tr>
<tr><td>Product Version</td><td colspan="2"></td><td>Document Revision Number</td><td>2.0</td></tr>
<tr><td rowspan="3">Evaluate this document</td><td colspan="4">Presentation:
(Introductions, procedures, illustrations, completeness, arrangement, appearance)
☐ Good ☐ Fair ☐ Average ☐ Poor</td></tr>
<tr><td colspan="4">Accessibility:
(Contents, index, headings, numbering)
☐ Good ☐ Fair ☐ Average ☐ Poor</td></tr>
<tr><td colspan="4">Editorial:
(Language, vocabulary, readability, clarity, technical accuracy, content)
☐ Good ☐ Fair ☐ Average ☐ Poor</td></tr>
<tr><td>Your suggestions to improve the document</td><td colspan="4">Please check suggestions to improve this document:
☐ Improve introduction ☐ Make more concise
☐ Improve Contents ☐ Add more step-by-step procedures/tutorials
☐ Improve arrangement ☐ Add more technical information
☐ Include images ☐ Make it less technical
☐ Add more detail ☐ Improve index</td></tr>
<tr><td colspan="5">If you wish to be contacted, complete the following:</td></tr>
<tr><td>Name</td><td colspan="2"></td><td>Company</td><td></td></tr>
<tr><td>Postcode</td><td colspan="2"></td><td>Address</td><td></td></tr>
<tr><td>Telephone</td><td colspan="2"></td><td>E-mail</td><td></td></tr>
</table>

Contents

Configuration Guide 6
Overview 6
Login 6
System Information 9
WAN Configuration 10
Supporting Devices 10
Configuration Wizard of Accessing WAN 10
WAN Interface Connection Information 14
DNS Server Configuration 14
E1 Configuration 14
Supporting Devices 14
E1 Port Configuration 15
E1 Service Configuration 17
DSP Service Configuration 18
Clock Source Configuration 19
E1 Group Configuration 21
Voice Configuration 27
Supporting Devices 27
Protocol Configuration 28
VoIP Port Configuration 39
Number Transform Configuration 46
Call Route Configuration 49
Black-white List Configuration 54
Call Service Configuration 57
Call Pickup Configuration 62
Group Ring Configuration 63
IVR System Configuration 65
Accounting Authentication Configuration 67
Fax Service Configuration 71
Other Configurations 73
Simulative Call Test 77
Voice Call Port Status 78
Current Call Communication Statistics 78
CSC Card Configuration 78

MTP/TUP Timer Configuration 79
Operation Status Monitoring 82
Operation Status Monitoring 82
Route Configuration 84
Supporting Devices 84
Static Route Configuration 84
System Management 85
Supporting Devices 85
Basic Information Configuration 85
Administrator Setting 86
Device Software Upgrade 86
Configuration File Management 88
Log Management 88
SNMP Parameter Configuration 90
Save Configuration 91
Typical Applications 93
Environment 93
Configuration Steps 94
Communication Configuration between Local and H323 94
Communication Configuration between FXS and PSTN 100
IP Fax Configuration 103

Configuration Guide

Overview

This chapter describes the web configuration of the VoIP gateway, including WAN configuration, E1 configuration, voice configuration, operation status monitoring, route configuration, and save configuration. The main interface of the WEB system comprises navigation bar and configuration interface.

📖 **Note**

The web configuration described in the chapter support Internet Explorer 6.0+.

Login

The WEB management system of the gateway supports the system administrator and common administrator.

VG6000 and VG6500 do not have the default user name or password, so you need to connect the gateway via telnet or Console port and then configure the login user in shell so that you can use the WEB management system normally. The following describes how to configure the shell commands of the user.

Configure the system administrator:

gateway#configure terminal //enter configuration mode
gateway(config)#user admin privilege 15 password 0 admin //configure the user with user name as admin, priority as 15, and password as admin; 15 is the highest priority

Configure common administrator:

gateway#configure terminal ///enter configuration mode

gateway(config)#user guest privilege 0 password 0 guest //configure the user with user name as guest, priority as 0, and password as guest; 0 is the lowest priority

The system administrator and common administrator correspond to different management authorities.

The authorities of the system administrator include the product information, WAN configuration, E1 configuration, voice configuration, operation status configuration, route configuration, system configuration and save configuration. The function navigation is as follows:

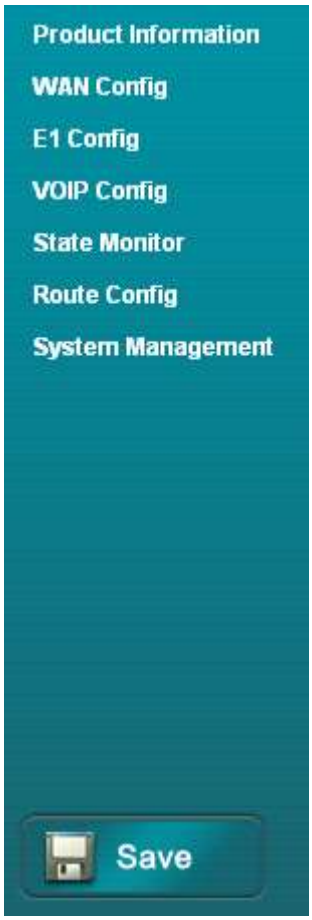


Figure 1-1 System administrator navigation

Caution

The above figure is the system administrator navigation of MyPower VG2000 (with E1), VGM6000, and VG6500.

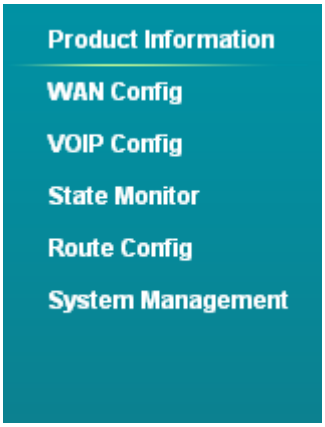


Figure 1-2 System administrator navigation

Caution

The above figure is the system administrator navigation of MyPower VG600 and VG800.

The authorities of the common administrator include system management (administrator settings) and save configuration.

The function navigation is as follows:

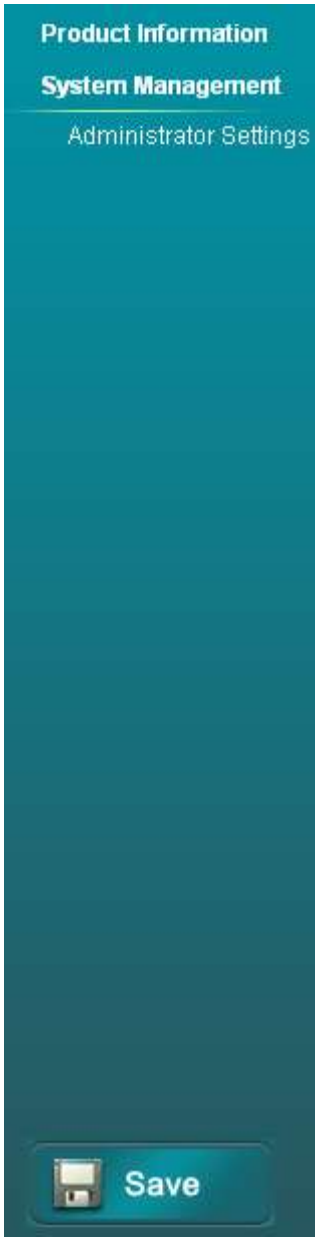


Figure 1-3 Common administrator navigation

System Information

You can view the current system information via **Navigation bar** > **Product Information**. The system information includes system ID, Monitor version information, IOS version, IOS file name, compiled time of IOS, WEB system version, and compiled time of WEB system.

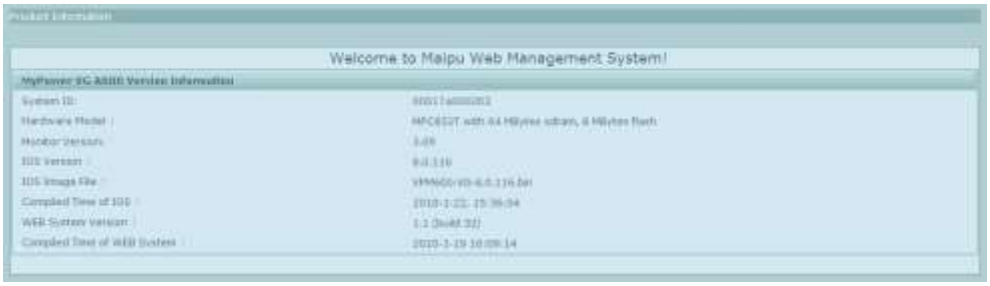


Figure 1-4 System information

Caution

The above figure is the system information of MyPower VGM6000.

WAN Configuration

Supporting Devices

MyPower VG A600, MyPower VG800, MyPower VG2000, MyPower VGM6000, MyPower VGM6500

Configuration Wizard of Accessing WAN

Enter the configuration wizard of accessing WAN from the navigation menu and configure the WAN access according to the wizard.

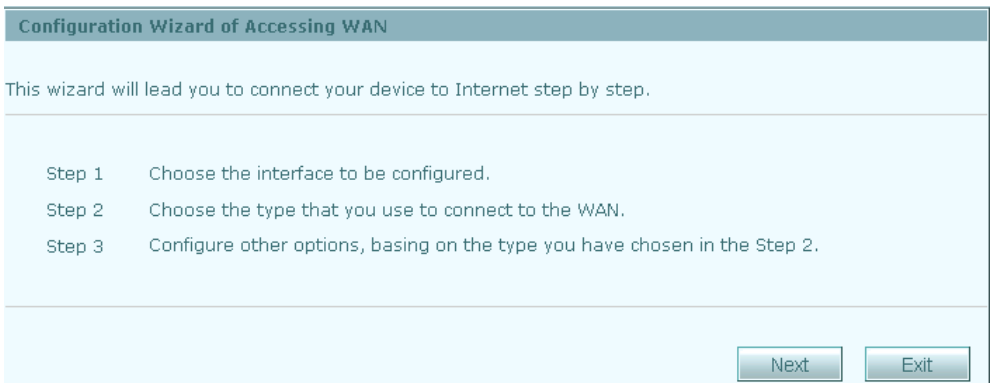

Configuration Wizard of Accessing WAN
This wizard will lead you to connect your device to Internet step by step.
Step 1 Choose the interface to be configured.
Step 2 Choose the type that you use to connect to the WAN.
Step 3 Configure other options, basing on the type you have chosen in the Step 2.
Next
Exit

Figure 1-5 Configuration wizard of WAN access

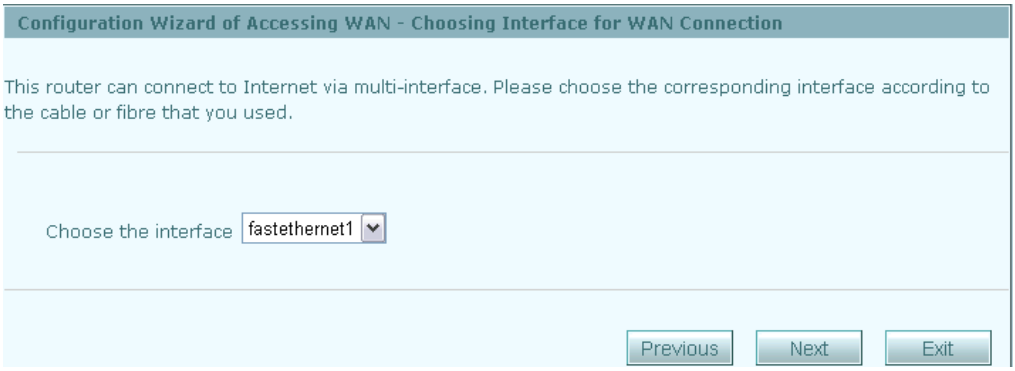

Configuration Wizard of Accessing WAN - Choosing Interface for WAN Connection
This router can connect to Internet via multi-interface. Please choose the corresponding interface according to the cable or fibre that you used.
Choose the interface
fastethernet1
Previous
Next
Exit

Figure 1-6 WAN connection interface

Figure 1-7 WAN access type

Caution

The above figure is the WAN access type of MyPower VG A600 and MyPower VG800.

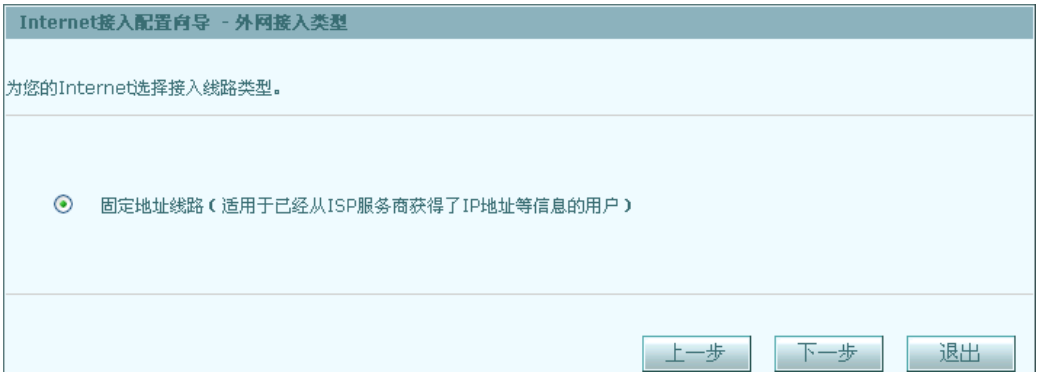


Figure 1-8 WAN access type

Caution

The above figure is the WAN access type of MyPower VG 2000.

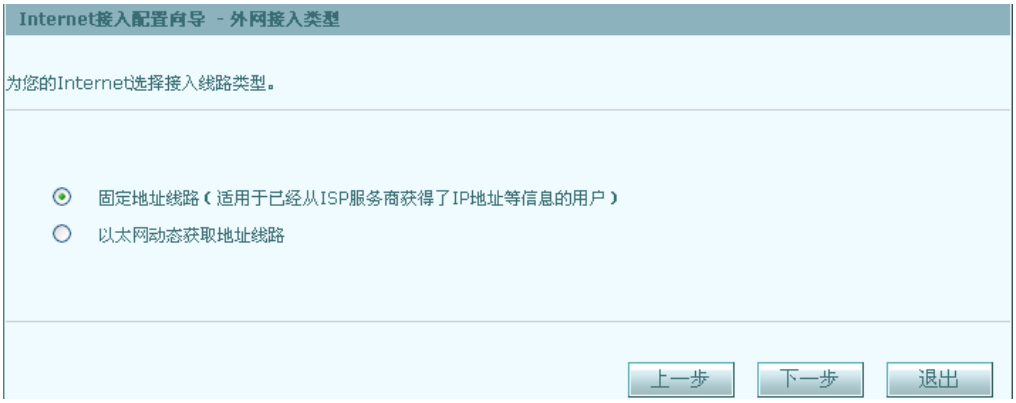


Figure 1-9 WAN access type

Caution

The above figure is the WAN access type of MyPower VGM 6000 and 6500.

WAN access line type: The WAN access lines of MyPower VG A600 and MyPower VG800 has three kinds of connecting Internet, that is, fixed address line, PPPoE dialup line, Ethernet dynamically getting address line. However, MyPower VG2000 has only one type of connecting Internet, that is, fixed address line. MyPower VGM6000 and 6500 has fixed address line and Ethernet dynamically getting address line. The following describes the three kinds of connecting Internet:

1. Fixed address line

The option means that the ISP that provides lines (such as China Telecom) provides the fixed IP address.

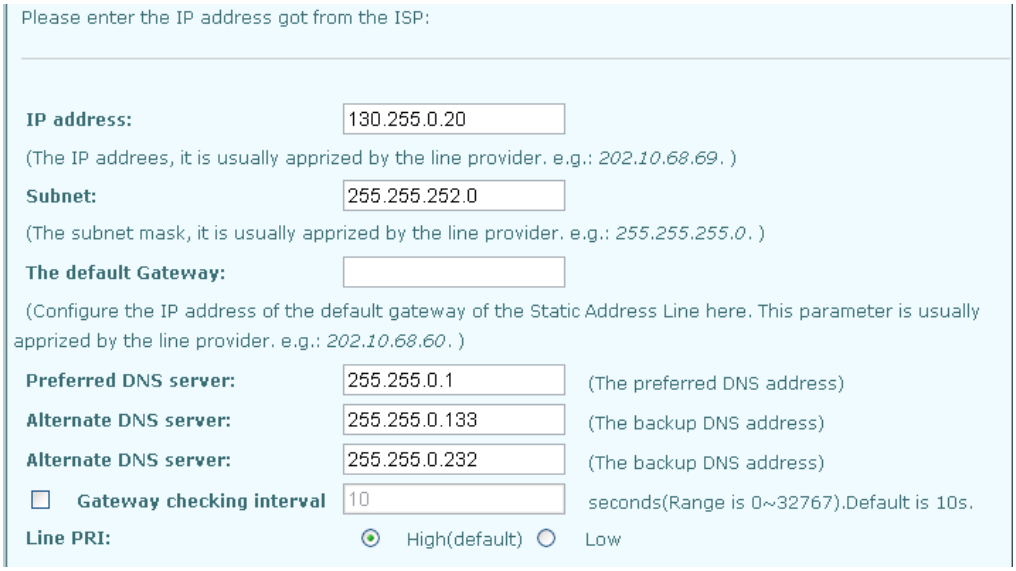

Please enter the IP address got from the ISP:
IP address: 130.255.0.20
(The IP addrees, it is usually apprized by the line provider. e.g.: 202.10.68.69.)
Subnet: 255.255.252.0
(The subnet mask, it is usually apprized by the line provider. e.g.: 255.255.255.0.)
The default Gateway:
(Configure the IP address of the default gateway of the Static Address Line here. This parameter is usually apprized by the line provider. e.g.: 202.10.68.60.)
Preferred DNS server: 255.255.0.1 (The preferred DNS address)
Alternate DNS server: 255.255.0.133 (The backup DNS address)
Alternate DNS server: 255.255.0.232 (The backup DNS address)
Gateway checking interval 10 seconds(Range is 0~32767).Default is 10s.
Line PRI: High(default) Low

Figure 1-10 Fixed address line

IP Address: The WAN IP address of the VoIP gateway provided by ISP.

Subnet Mask: The WAN subnet mask of the VoIP gateway provided by ISP; the user can get it from ISP.

Default Gateway: It is provided by ISP. The user can get if from ISP.

Preferred/Alternate DNS server: It is provided by ISP. The user can get if from ISP.

Gateway Detection Interval: On the basis of this function, the equipment will send message regularly to check whether WAN link is normal.

Line Priority: Configure the management distance of the default route to realize the route forwarding.

2. PPPoE dialup line

This option indicates PPPOE dial-up to internet.

Figure 1-11 PPPOE dailup line

User name: It is provided by ISP. You can get it from ISP.

Password: It is provided by ISP. You can get it from ISP.

Caution

PPPOE takes default autodial mode. Before using this function, the user has to apply for ADSL service from Telecommunication Office, so as to get username and password for accessing Internet.

3. Ethernet Dynamic Address Line

This option indicates that the user shall get and configure IP address and subnet mask of external network port of the gateway by configuring DHCP Client dynamically.

WAN Interface Connection Information

You can view the current WAN configuration and connection information of the VoIP gateway.

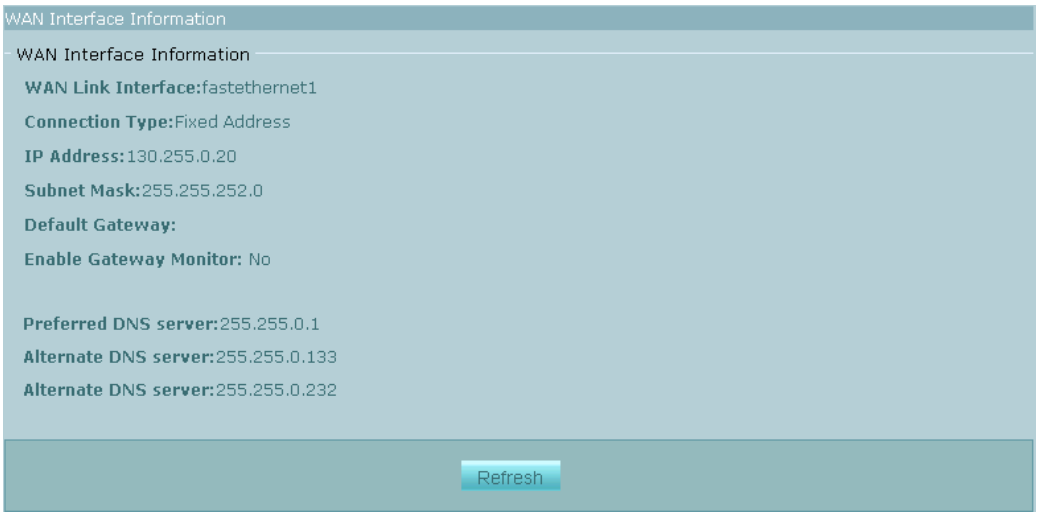


Figure 1-12 WAN port connection information

DNS Server Configuration

The user can set global DNS server address for gateway on the interface.

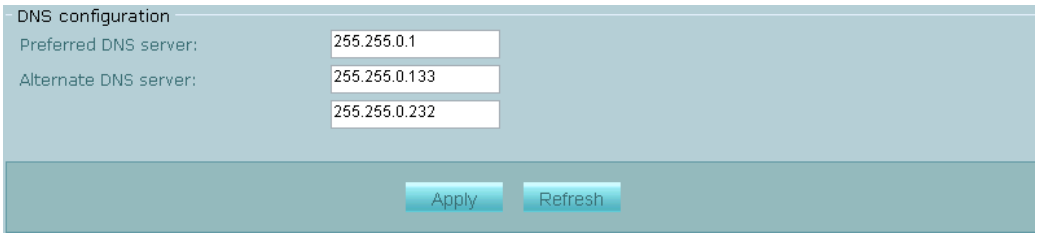


Figure 1-13 DNS server configuration

E1 Configuration

Supporting Devices

MyPower VG2000, MyPower VGM6000, MyPower VGM6500

E1 Port Configuration

The following is the interface for configuring the protocol bound to the E1 port.

E1port binding PRI protocol:

Figure 1-14 E1port configuration

Caution

The above is the E1 port configuration of MyPower VGM6000 and 6500.

Figure 1-15 E1 port configuration

Caution

The above figure is the E1 port configuration of MyPower VG2000.

Set pri signal channel at the 16th timeslot: Configure the signal timeslot on E1. Currently, you can only configure the 16th timeslot as the signal timeslot.

Listen to Ringback: whether to listen to the remote ringback.

Play Ringback: Whether to play ringabck for the remote.

ISDN type: Configure PRI direction. When using PRI for communication, one end should be USER and the other end should be NET;

Enable E1 clock as system clock source of gateway: The configuration is valid only for VG2000. The requirement of the R2 protocol for system clock is high. To avoid that the error code on the line causes the call failure, you need to configure the system clock correctly. When

two gateways are connected via E1 and are bound to the R2 protocol, the clock of one gateway is configured as the internal clock and the clock of the other gateway needs to be configured as the E1 follow clock. When binding the PRI protocol, you need to configure the E1 clock source, avoiding that the services (such as fax) cannot be used or the access rate is low. After switching E1 and binding the protocol, you need to re-set the E1 clock as the internal clock.

E1 port binding R2 protocol:

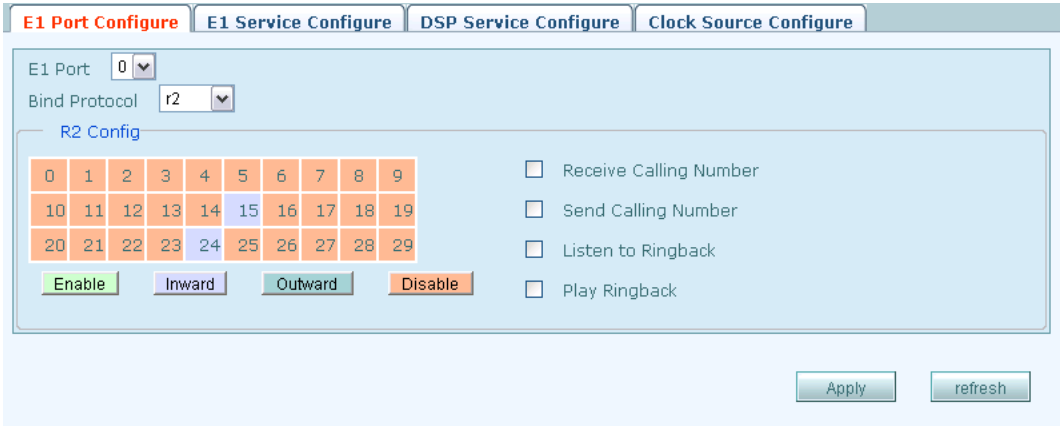


Figure 1-16 E1 port configuration

Caution

The above figure is the E1 port configuration of MyPower VGM6000 and 6500.

Figure 1-17 E1 port configuration

Caution

The above figure is the E1 port configuration of MyPower VG2000.

■: Enable the selected channel;

■: Enable the selected channel and set it as the inward trunk;

■: Enable the selected channel and set it as the outward trunk;

■: Disable the selected trunk;

Receive calling number: Whether to receive the caller number;

Send calling number: Whether to send the caller number;

Listen to ringback: Whether to listen to the remote ringback;

Play ringback: Whether to play the ringback to the remote;

E1 Service Configuration

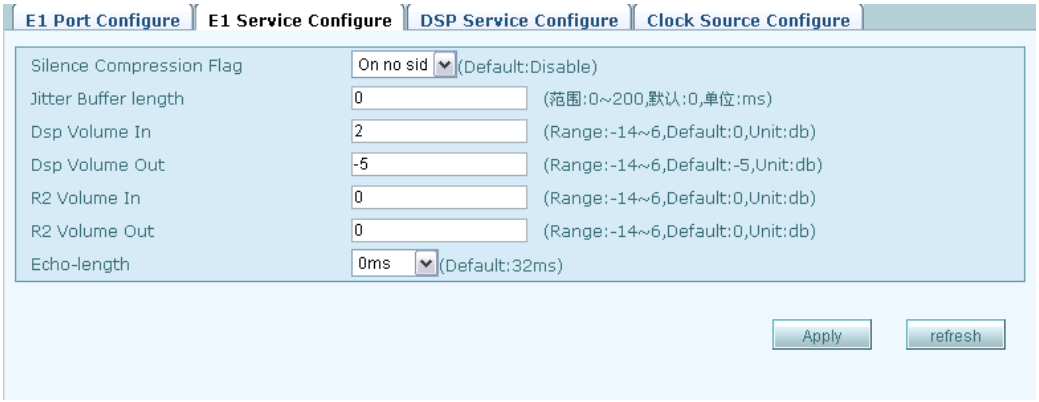


Figure 1-18 E1 service configuration

Caution

The above figure is the E1 service configuration of MyPower VGM6000 and 6500.

Figure 1-19 E1 service configuration

Caution

The above figure is the E1 service configuration of MyPower VG2000 (with E1 card).

Silence compression flag: There are four options, that is, {disable| nosid | sid | pt13}:

Disable: Disable the silence compression function;

Nosid: Do not send the silence packet;

Sid: Send the sid frame:

pt13: Send the sid frame; the sid frame is expressed by 13; the option is valid only for g711;

Jitter buffer length: Configure the time of removing the jitter; when the network jitter is large, the order of receiving the voice packets may be inconsistent with the order of sending the voice packets, which causes the jitter. To remove the jitter, adopt the jitter buffer technology at the receiving end and the length of the jitter buffer is the maximum time of removing the jitter. For example, if setting the length of the jitter buffer as 20ms, the receiving end can re-range the voice packets received within 20ms and then play them, so as to remove the jitter within the time period.

DSP volume in/out: Configure the global DSP volume; the negative means reducing and the positive means increasing. DSP input volume controls the signal gain from PCM; DSP output volume controls the signal gain output to PCM.

R2 volume in/out: Configure the output/input gain of receiving r2 signal;

Echo length: Configure the global echo cancellation length (valid for MyPower VGM6000 and VGM6500).

DSP Service Configuration

When the DSP channels do not correspond with the voice channels one by one, you can configure the DSP convergence to protocol some channels and play busy tone for the new incoming call when DSP channels are not enough. After enabling the function, the DSP resources reserved for E1 can be used only by the calls via E1 and the other calls can only use the other DSP channels, that is, the calls via E1 trunk has the highest priority.

After enabling the function, the gateway first assigns one DSP to play the busy tone. Therefore, if the new calls can be distributed with DSP, the gateway connects the timeslot with the DSP for playing the busy tone and

the user hears the busy tone. When the function is disabled or the calls cannot be distributed with DSP, the user cannot hear any sound.

Figure 1-20 DSP service configuration

Caution

The above figure is the DSP service configuration of MyPower VG2000.

Figure 1-21 DSP service configuration

Caution

The above figure is the DSP service configuration of MyPower VGM6000 and 6500.

Clock Source Configuration

The following is the interface for configuring the work mode of the clock source as the priority. The function is valid only for MyPower VGM6000 and VGM6500.

Figure 1-22 Clock source configuration

When clicking , display as follows:

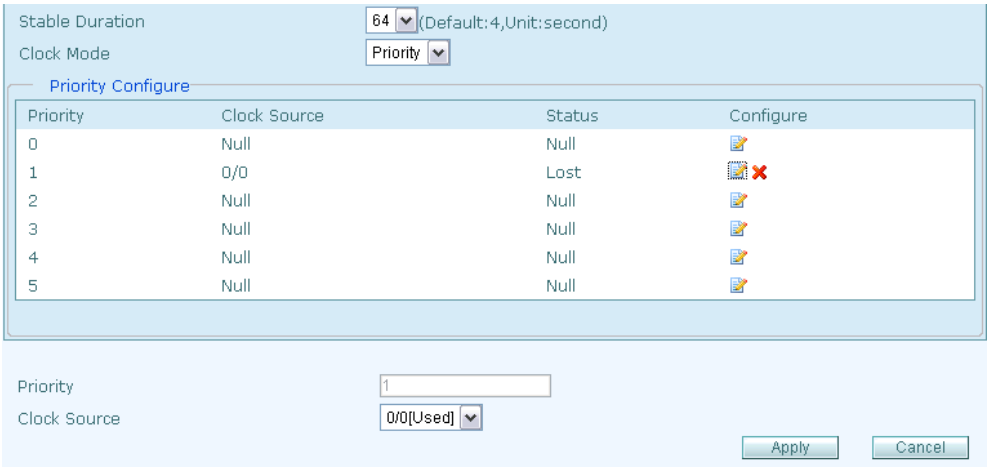


Figure 1-23 Edit the priority configuration

Caution

When the work mode of the clock source is priority and the mode of configuring priority 0 is BITS, edit the priority 1. If the selected mode is used, the system prompts "the mode is occupied".

Click to delete the corresponding item. After deleting successfully, display as follows:

Priority	Clock Source	Status	Configure
0	Null	Null	
1	Null	Null	
2	Null	Null	
3	Null	Null	
4	Null	Null	
5	Null	Null	

Figure 1-24 Priority configuration

Caution

When the work mode of the clock source is priority and the priority 0-5 is set as null, the device automatically modifies the work mode of the clock source to specify and the specified mode is modified to **Local**, as follows:

Figure 1-25 Clock source configuration

E1 Group Configuration

This section describes the configuration of the E1 group. By configuring E1 group, the local VoIP gateway based on the No. 7 signal can exchange signals with the destination VoIP device.

Create E1 Group

The gateway with E1 module can perform the E1 group configuration (such as VG2000 and VGM-6xxx). The configurations of the E1 group and No. 7 signal cannot be performed on the gateway without E1 module.

Caution

Each E1 group should contain at least one E1 port. One E1 port cannot be contained in two different E1 groups. One VoIP gateway device can be configured with the same E1 groups as the E1 ports at most.

The created E1 group list is as follows:

Figure 1-26 E1 group configuration

E1 Group Configuration

The interface for configuring the E1 group:

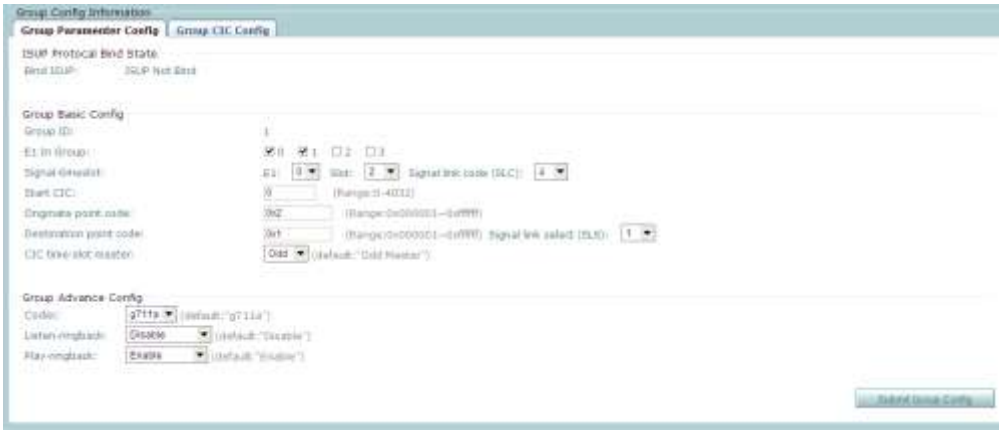


Figure 1-27 E1 group configuration parameter (after selecting “bind ISUP”)

Figure 1-27 E1 group configuration parameter (after selecting “bind TUP”)

E1 group information configuration includes E1 group configuration parameter and E1 group CIC configuration. E1 group configuration parameter includes basic configuration and extended configuration (if the user selects Bind TUP in the bound protocol list, add one TUP additional configuration). The group basic configuration can be changed only when the ISUP and TUP are not bound, while the group extended configuration and TUP additional configuration can be modified when the protocol is bound. The group basic configuration, extended configuration or TUP additional configuration is unique in the group, while you can configure

multiple the group CIC configurations according to different CIC configuration types. Same as the group basic configuration, E1 group CIC configuration can be modified only when the protocol is not bound.

The following describes the configuration items:

Basic configuration of E1 group:

Group ID: The ID of the E1 group can be specified when creating the group;

E1 in group: Specify which E1 ports the E1 group should contain;

Caution

1. The E1 port added to other E1 groups cannot be added repeatedly;
2. The E1 port bound with PRI or R2 protocol can be added to E1 group, but when binding protocol, it results in failure.

Signal-timeslot: Specify the timeslots used to exchange signals with the destination device in E1 group;

Signal link code: Specify the flag code of the signal link used to exchange the signals with the destination device in E1 group;

Start CIC: The start CIC of the E1 group; the range is (0 ~ 4064-(the number of E1 in E1 group-1) *32).

Originate point code: The local signal point code of E1 group and the range is 0x000001~0xffffff;

Destination point code: Specify the destination signal point code and the range is 0x000001~0xffffff;

Signal link select: Specify the selecting code of the destination signal link and the range is 0-15.

Caution

1. Destination point code and signal link code should keep consistent with the destination device. Otherwise, the signals cannot be exchanged normally (for example, the call cannot be connected);
2. Destination point code cannot be consistent with local point code.

CIC time-slot master: Configure the CIC timeslot master of E1 group; by default, it is odd;

Group advance configuration:

Codec: Configure the voice code of the E1 group; the default value is g711a;

Listen to ringback: Configure the E1 group to listen to the remote ringback; by default, it is disabled;

Play ringback: Configure E1 group to play the ringbacl to the remote; by default, it is enabled;

TUP additional configuration:

Overlap receiving number: Configure the overlap receiving number when binding the TUP protocol; by default, it is disabled;

Initial address message: Configure the initial address message of E1 group when binding TUP; the default value is iai;

Subsequent address message: Configure the subsequent address message of the E1 group when binding the TUP protocol; the default value is sam;

Hang-up control mode: Configure the hang-up control mode of E1 group when binding the TUP protocol; the default value is caller.

Group CIC configuration:

The interface for the CIC configuration of E1 group:

Figure 1-28 E1 group CIC configuration

The CIC configuration of E1 group should be consistent with the CIC configuration of the destination device.

Usually, the configuration corresponding relation is one complicated process. To facilitate the user configuration, Maipu VoIP gateway realizes three configuration modes (based on E1 group, based on E1 and based on timeslot).

CIC based on E1 group: Configure CIC based on E1 group; the mode includes increase and decrease;

CIC based on E1: Configure CIC based on E1; the parameters to be configured include E1, mode and start CIC;

Decrease: The specified start CIC value minus the start CIC of the group basic configuration should be 31/63/95/127 so that the configuration can succeed.

Increase: The specified start CIC value minus the start CIC of the group basic configuration should be 0/32/64/96 so that the configuration can succeed.

CIC based on timeslot: Configure the CIC based on timeslot; the parameters to be configured include E1, timeslot, mode and start CIC;

You can specify the start CIC at random, but the value should be within the configuration range of the start CIC of group basic configuration.

Caution

The CIC range should be within the range of the start CIC of the E1 group. The CIC range of E1 group is from startcic to startcic+(the number of E1 in E1 group) × 32-1.

E1 Group Protocol Binding

Currently, ISUP and TUP can be bound. The user can select the desired protocol above E1 group configuration parameter (the options include not bind, bind ISUP and bind TUP). After selecting "Bind ISUP" (or "Bind TUP", the lower part of the interface displays the corresponding "Bin ISUP" (or "Bind TUP") button. Before clicking the button, no protocol is bound actually.

After configuring E1 group parameters and E1 group CIC, click "Bind ISUP" (or "Bind TUP") and the system prompts success. If the E1 group and E1 group CIC are not configured correctly, the system prompts failure. After binding successfully, you can click "View CIC state information" to view the CIC status.

View E1 CIC Status

The interface provides the query and filtering of the CIC normal status and detail status, as shown in the following figure:

Figure 1-29 CIC status (normal)

View and filter the CIC normal status:

For example, when the user selects **CIC time-slot master** as **All**, click **Do Filter**, as follows:

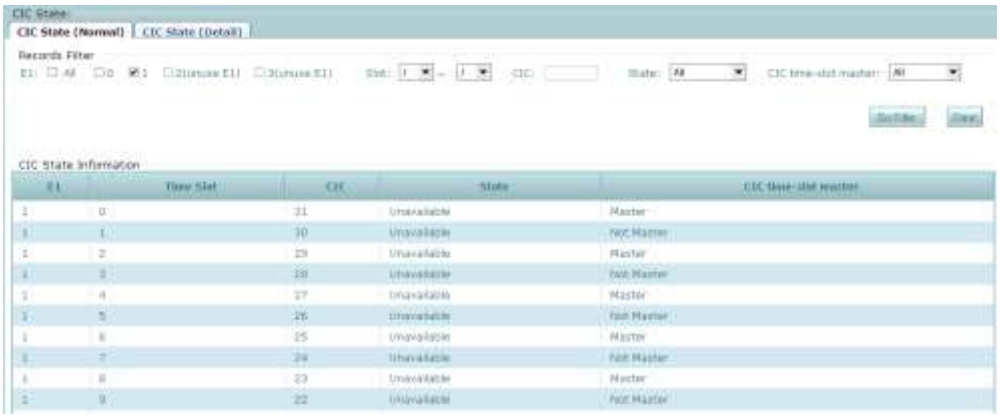


Figure 1-30 CIC status (normal)

When clicking **Clear**, the following interface is displayed:

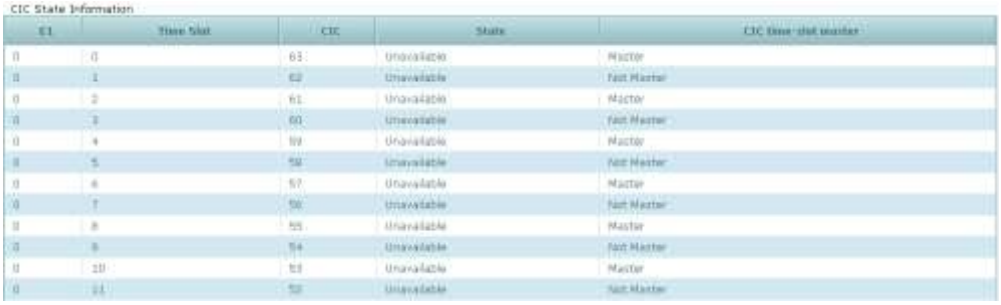


Figure 1-31 CIC status (normal)

View the details of the ISUP CIC status:

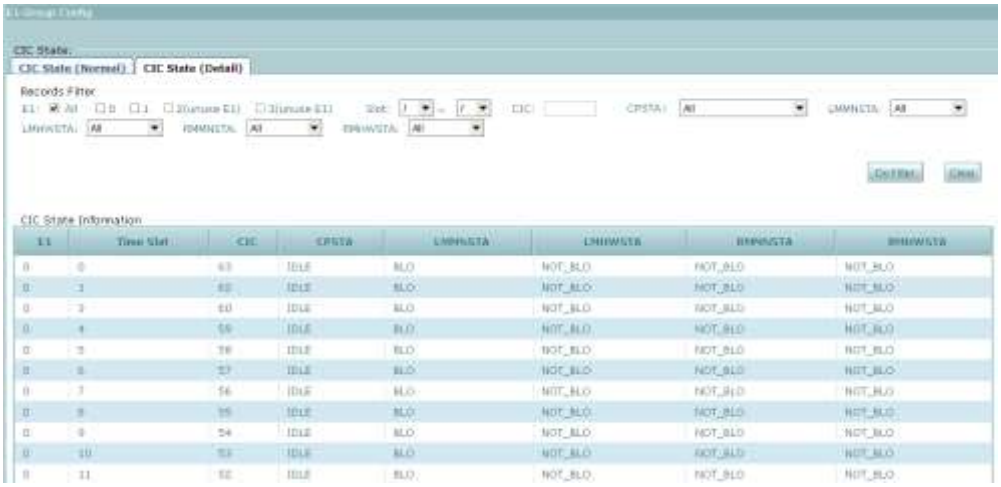


Figure 1-32 ISUP CIC status (detail)

View the TUP CIC detail status:

Figure 1-33 TUP CIC status (detail)

Voice Configuration

Supporting Devices

MyPower VG A600, MyPower VG2000, MyPower VG800, MyPower VGM6000, MyPower VGM6500

Protocol Configuration

Currently, the voice gateway can only run either of H.323 protocol and SIP protocol. The voice protocol can only be bound with the communication interface with the IP address.

If the current interface is configured with the H323 protocol, the process of switching to the SIP protocol is:

1. First switch "Protocol" from "H.323" to "Null", which removes the H.323 protocol from the binding interface;

2. And then switch from "Null" to "SIP". After switching to the interface of configuring the SIP protocol, first select the binding interface. Otherwise, the setting cannot take effect. After setting the other options of the SIP protocol, click "Set" and switching to SIP succeeds.

The process of switching from SIP to H323 is similar.

If the selected is H.323 protocol, the protocol configuration interface is as follows:

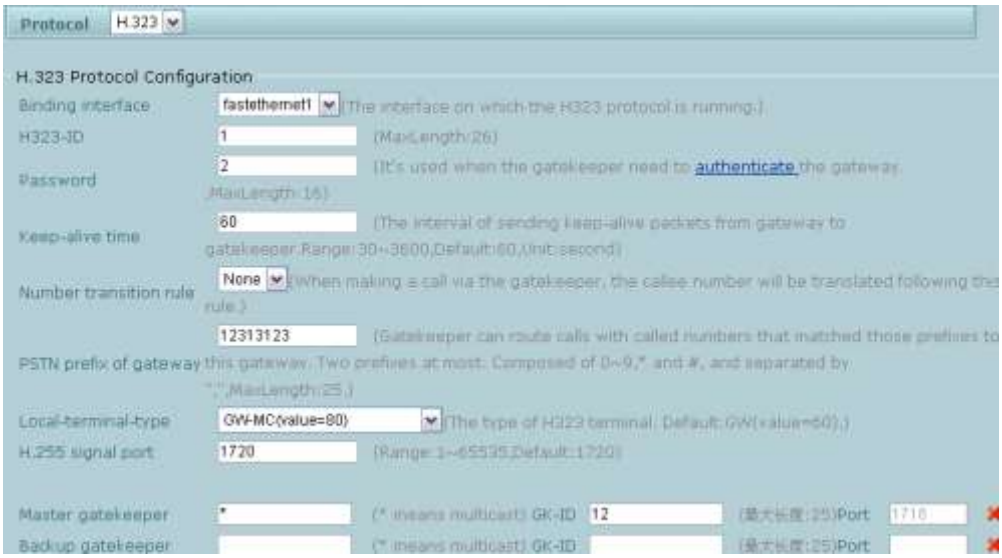


Figure 1-34 H323 protocol

Binding interface: Specify the interface as the interface as the running interface of the H323 protocol on the voice gateway;

H323-ID: Used by the gatekeeper to identify the gateway interface (optional);

Password: The password for the authentication between the gateway and gatekeeper. The option is needed to be filled according to the user name

and password of the gatekeeper only when the gatekeeper and the gateway need the authentication (optional).

Keep-alive time: The interval of the gateway sending the keepalive packets to the gatekeeper; the value range is 30~3600s. The default value is 60s;

Number transition rule: The called number is transited according to the selected number transition rule when calling via the gatekeeper. For the number transition rule, refer to Voice Configuration ->Number transition configuration (Optional configuration, used for irregular voice number design. Leave it unused, or result in failed calling. For application, please make confirmation about it with Tech Service Department of Maipu Communication Co., Ltd.)

PSTN prefix of gateway: Used by the gatekeeper to process the call route, that is, the telephone number beginning with the prefix is routed by the gatekeeper to the gateway. You can configure two technical prefixes at most. It comprises the numbers, * and #, and is separated by, (optional; if the gateway does not provide the PSTN grounding for the other gateways in the network, the option should not be configured).

Local-terminal-type: The type of the entity in the H.323 network, reflecting the terminal performance. The priorities of the terminal types in H.323 from high to low are MCU, gatekeeper, gateway, terminal, and MC+MP, MC unit to the unit without MC or MP (optional);

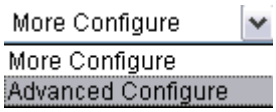
Master gatekeeper/backup gatekeeper: Input the master gatekeeper IP, domain name or * (* means to search the gatekeeper by multicast) (optional, if the gatekeeper networking is not used, the option does not need to be configured. To initiate the IP call, initiate the call via the VoIP dialer configured in the call route).

GK-ID: It means the domain of the gatekeeper device (mandatory information for registering the gatekeeper; it should be got by the gatekeeper administrator). You can input -, which means the first domain registered to the gatekeeper by default.

Port: The port discovering the gatekeeper; the default value is 1718;

Register to gatekeeper: If register is enabled, first the function of making call via the gatekeeper can be realized. Besides, with registration, the gatekeeper can complete the unified management for some functions of all terminals in the managed H.323 network system, such as bandwidth management, load balance, authentication management, and active/standby switchover. The right yellow words of the option indicate whether the current gateway is registered to the gatekeeper successfully.

Click ✕ to delete the gatekeeper configuration.



Click and you can enter the H.323 advanced configuration interface, as follows:

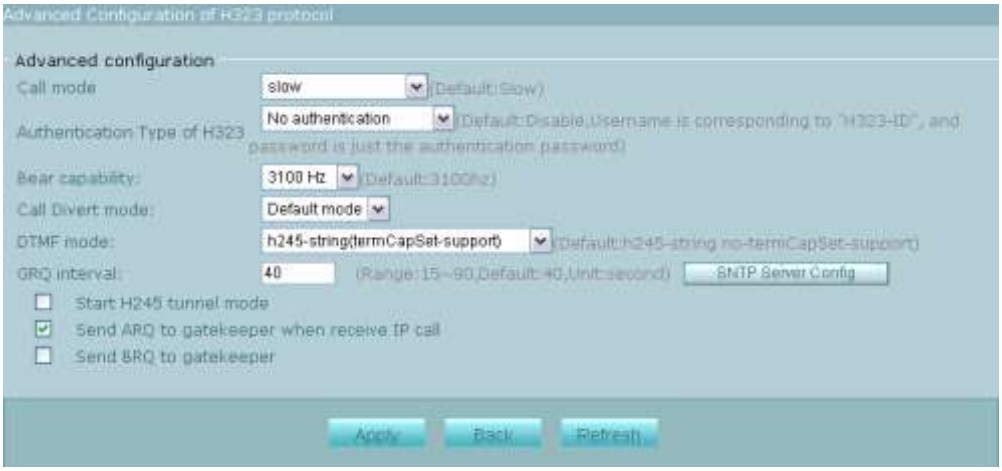


Figure 1-35 H323 protocol advanced configuration

Authentication Type of H323: The authentication mode for the gatekeeper during the H.323 registration or call, including H235 CAT, H235 CAT FOR CISCO, H235 ANNEXD, H235 SIMPLE MD5 and Maipu private authentication mode. By default, do not enable authentication.

Combing the authentication setting of the device with the authentication function of the gatekeeper can improve the security of the H.323 network, realize the authorization and limitation of the gatekeeper for the gateway device, and strengthen the management capability of the gatekeeper for each H.323 terminal or even the whole H.323 network.

Here, the user can also configure the SNTP server. The SNTP configuration is to make all devices taking part in the authorization and authentication get the unified network time, because the time authentication is an important step in the authentication.

Bear capability: The bear capability of the H.323 voice; the configuration is to strength the compatibility with the devices of other manufacturers.

Call Divert Mode: Select call forward mode, including two modes. One is to encapsulate the call forward information in the 450 message; the other is to carry call forward message in the facility message. The default value is the latter mode.

DTMF mode: The sending mode of the DTMF signals; **H.245-string**-the DTMF signals are transmitted on the H.245 connection; **Q931-keypad**-the DTMF signals are transmitted on the H.225 connection; **RTP-NTE**: Adopt the RTP packets complying with the RFC2833 protocol to send the DTMF signals. You can set the dynamic payload type. The default value is 101. The dynamic payload type can be different from the payload type of the RTP fax mode of T38.

Selecting H.245-string means to use the H.245 connection to transmit the DTMF signals. H.245-string (do not judge the peer capability set) means that if the peer terminal capability set does not contain the H.245-string

capability, the local still can send the DTMF signals on the H.245 connection via the configuration. H.245-string (judge the peer capability set) means that the H.245 connection can be used to transmit the DTMF signals only when the peer terminal capability set contains the H.245-string capability.

GRQ interval: The interval of sending GRQ when the gateway tries to register the gatekeeper;

Start H245 tunnel mode: Whether to use the tunnel mode to set up the call. The tunnel mode is to encapsulate the H.245 message in the H.225 message to send. It is used when setting up connection quickly and the fax is needed.

Send ARQ to gatekeeper when receive IP call: Whether to send ARQ messages to the gatekeeper when the gateway serves as the called;

Send BRQ to gatekeeper: Whether to send BRQ to the gatekeeper if the code mode changes, which is enabled when combing with the gatekeeper bandwidth management.

Click SNTP Server Config and the system displays, as follows:

Figure 1-36 SNTP server configuration

To switch to the SIP protocol, enter the **Protocol Configuration** interface and select the running protocol of the device as none. First, stop the current H323 protocol. After clicking **OK** to remove the H.323 protocol successfully, select **SIP** and the interface of configuring the SIP protocol is displayed as follows:

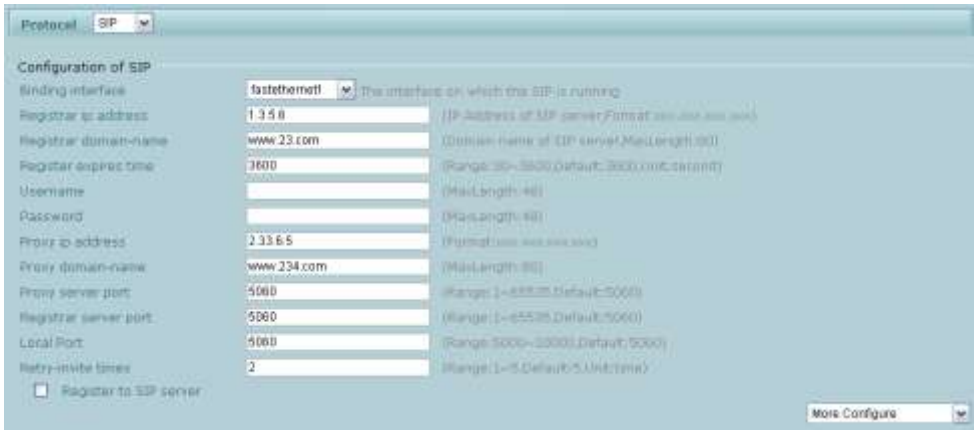


Figure 1-37 SIP protocol configuration

Binding interface: Specify the running interface of the VoIP gateway SIP protocol (mandatory; select the interface according to the VoIP application environment);

Register ip address: The address of the SIP registration server (optional);

Register domain-name: The domain name of the SIP registration server (optional; to use the option, ensure that the configured DNS server can resolve the domain name);

Register expires time: The value range is 200- 3600s and the default value is 3600s (optional);

Username/password: The user name and password for logging into the SIP server (optional; if the SIP server needs to authenticate the SIP terminal, the user name and password are provided by the SIP server administrator);

Proxy ip address: After configuring the option, the SIP signaling on the device is transferred by the server;

Proxy domain-name: Configure the domain name of the proxy server (optional; to use the option, ensure that the configured DNS server can resolve the domain name);

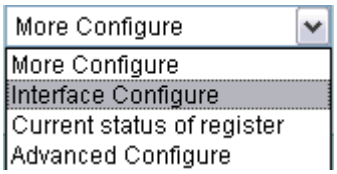
Proxy server port: Specify the port of the remote proxy server and the default value is 5060;

Register server port: Specify the port of the remote register server and the default value is 5060. It can use the same port with the proxy server.

Local port: Configure the local port number used by the SIP protocol;

Retry invite times: Specify the times of re-transmitting the INVITE message when initiating the call;

Register to SIP server: Ticking the check box means to enable the gateway to register to the SIP server. The registered telephone number of the local gateway is registered to the SIP server;

Select 

and you can view the sub interface configuration information, as follows:

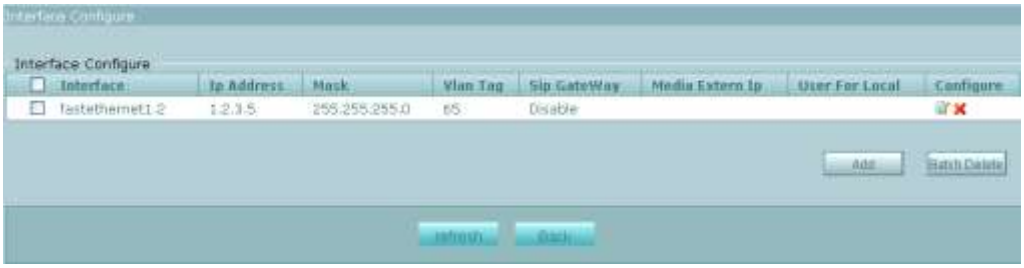


Figure 1-38 Sub interface configuration information

Click **Add**:

Figure 1-39 Add sub interface configuration

Interface: Configure the sub interface range;

IP address: Configure IP address;

Mask: Configure subnet mask;

Vlan Tag: Configure Vlan Tage;

Sip gateWay: Enable or disable the SIP protocol;

Media Extern Ip: Configure the uplink IP address;

User for Local: Set with the uplink IP address;

Click **Edit**:

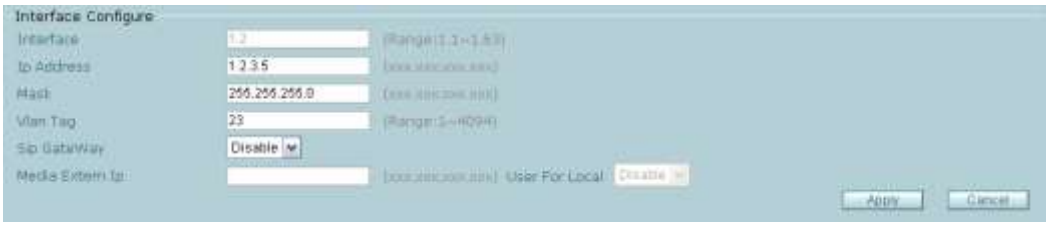
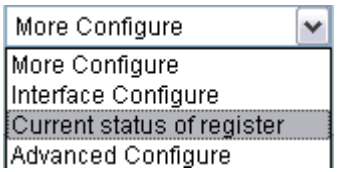


Figure 1-40 Edit sub interface configuration

is used to delete one sub interface configuration. Select the check box before the interface, click **Batch delete** and you can delete the configuration information of multiple sub interfaces.

Refresh: Refresh the current interface;

Back: Return to the previous interface;

Select 

and you can view the current registration status information, as follows:

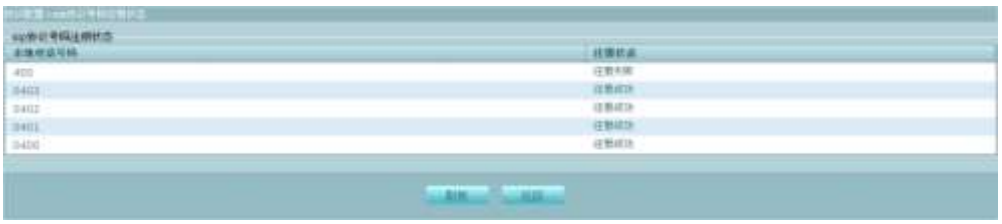
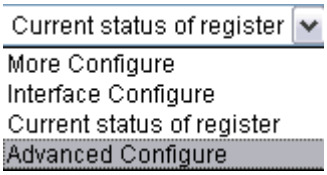


Figure 1-41 SIP protocol number registration status

Select 

to enter the advanced configuration interface of the SIP protocol, as follows:

Figure 1-42 SIP protocol advanced configuration

Caution

The above is the SIP protocol advanced configuration of MyPower VGM6000 and 6500.

Figure 1-43 SIP protocol advanced configuration

Caution

The above figure the SIP protocol advanced configuration of MyPower VGA600, VG800, and VG2000.

DTMF sending mode: INFO message mode adopts the INFO method of the SIP protocol to send the DTNF information; RTP-NTE mode adopts the RTP packet complying with the RFC2833 protocol to send the DTMF information. You can set the dynamic payload type and the default configuration is 101. The dynamic payload type cannot be the same as the payload type of the T38 RTP fax mode. You can also set the INBAND mode to send the DTMF information.

Sip Refer: You can select carrying the tdialog field or replaces field;

Timer_Z: Configure the timer-Z;

National Code: Configure the country code;

Area code: Configure the area code;

Session Time: Enable or disable the call keepalive function;

Session-Expires: Configure the Session-Expires time;

Min-SE: Configure the Min-SE time;

Force Update: Enable or disable force keepalive function;

Session-Expires Refresher: Configure the Refresher parameter of Session-Expires;

Priority mode: Configure the dynamic fax negotiation priority mode, including T38 or Pass Through (only 6000 and 6500 have the function);

Prack: Whether to enable the prack function;

Dynamic Fax: Whether to enable the dynamic fax function (only 6000 and 6500 have the function);

NAT configuration:

Enable STUN client: Select the check box to enable the STUN client. To enable the STUN client, you need to select the interface bound to the STUN protocol from the "Binding interface" drop-down list.

Primary STUN server status: Display the running status of the primary STUN server. The STUN server has the Active and Blocked states;

Primary STUN server domain name: Configure the domain name of the primary STUN server;

Primary STUN server IP address: Configure the IP address of the primary STUN server;

Primary STUN server port: Configure the port of the primary STUN server;

Backup STUN server status: Display the running status of the backup STUN server. The STUN server has the Active and Blocked states;

Backup STUN server domain name: Configure the domain name of the backup STUN server;

Backup STUN server IP address: Configure the IP address of the backup STUN server;

Backup STUN server port: Configure the port of the backup STUN server;

NAT type auto-detect period: The period of the STUN client detecting the NAT type automatically;

NAT keep alive time: The mapping update time; set the time of updating the public network mapping address at the local;

Current type of NAT: Display the current NAT type; the **Detect NAT type** button is used to detect the NAT type manually.

🕮 **Note**

When using the **Detect NAT type** button to detect the NAT type manually, ensure that the current mapping on NAT is deleted. Otherwise, maybe the detection result becomes wrong.

If **NAT type auto-detect period** is smaller than the NAT mapping timeout time on NAT, the detection result may become wrong, but do not affect the NAT function of the UDP packet.

When enabling the STUN client, do not need to perform Traversing Static NAT Configuration.

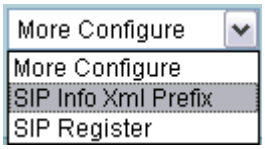
Figure 1-44 Abroad configuration

Media IP: The external address of the media when configuring NAT traversal;

User For Local: Enable or disable the local using function;

Signal IP: The external address of the SIP signaling when configuring NAT traversal;

Start Register Domain Name SRV Query: Configure starting the register domain name SRV query;

Select 

to enter the interface of configuring the SIP service number prefix, as follows:

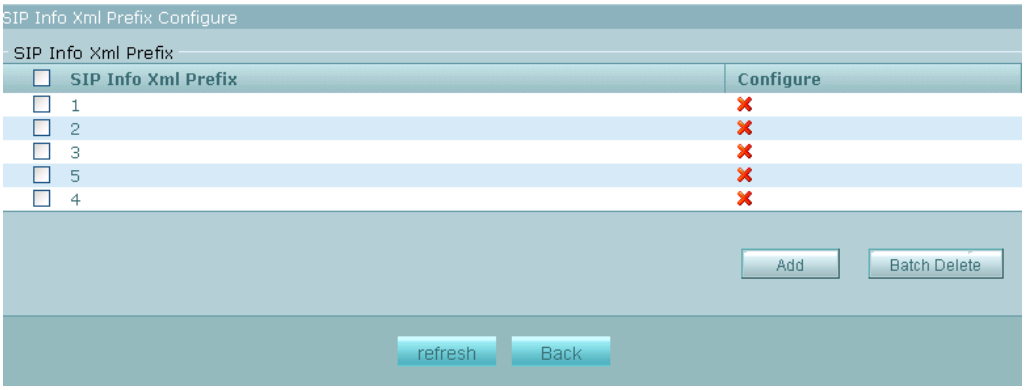


Figure 1-45 SIP service number prefix

Click **Add**:

Figure 1-46 Add SIP service number prefix

SIP Info Xml Prefix: Configure the SIP service number prefix, comprising up to eight bits;

is used to delete one SIP service number prefix. After selecting the check box before the SIP service number prefix, click **Batch Delete** and you can delete multiple SIP service number prefixes.

Refresh: Refresh the current interface;

Back: Return to the previous interface.

Select

to enter the SIP register group configuration interface, as follows:

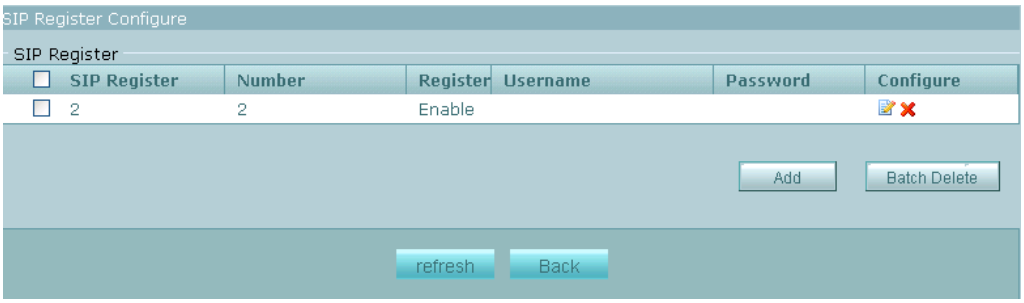


Figure 1-47 SIP register group

Click **Add**:

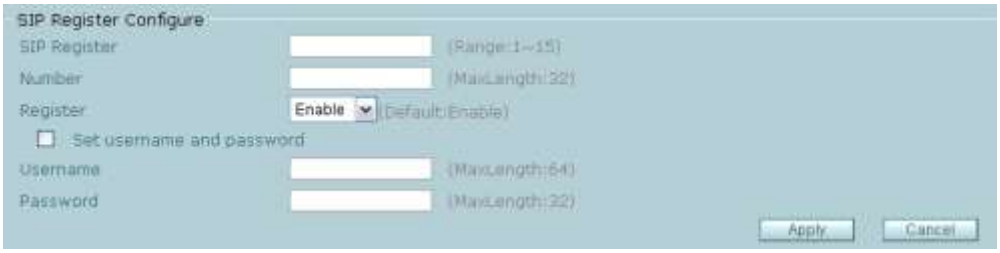


Figure 1-48 New SIP register group

SIP Register: Configure the SIP register group number;

Number: Configure the phone number;

Register: You can select Enable or Disable;

User name and Password: Before configuration, you need to select the check box before **Set username and password**;

Caller transit rule: Configure the caller transit rule;

is used to delete one SIP register group. Select the check box before SIP register group, click **Batch Delete** and you can delete multiple SIP register groups;

Refresh: Refresh the current interface;

Back: Return to the previous interface.

VoIP Port Configuration

Enter the interface and you can view and edit the number and port status configured on all VoIP ports.

Figure 1-49 Voice port configuration

Select different card number and ths system displays different port number.

Click ✚ to add the telephone number for the specified port.

Click **Configure** to change the telephone number; click **Delete** to delete the number.

Caution

The number of the FXO port can be configured as "x."; x means any one number; . means one or multiple numbers. For example, FXO can configure the number as 9xxxxxxxx, which means that the 9-digital number beginning with 9 makes call via the FXO interface. For more number policies, such as the number transition, whether to register the gatekeeper and the adopted code, enter the POTS dialer interface of the call route configuration to configure.

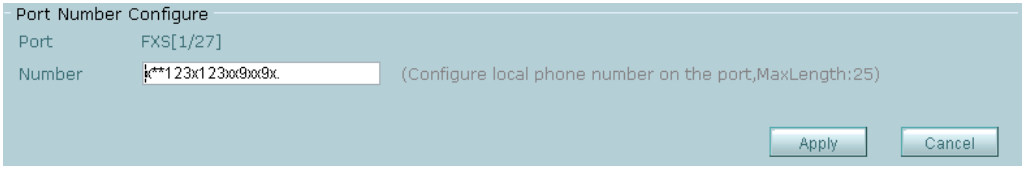


Figure 1-50 Port number configuration

Select the check box before the port, click **Advanced Configuration** to enter configuration of the physical features of the port and other advanced configuration.

The interface of configuring the FXS port is as follows:

Figure 1-51 FXS port advanced configuration

Caution

The above is the FXS port advanced configuration of MyPower VGA600, VG800, and VG2000.

Figure 1-52 FXS port advanced configuration of MyPower VGM6000 and 6500

Caution

The above is the FXS port advanced configuration of MyPower VGM6000 and 6500.

Port: Display the voice port to be configured;

Enable: Configure port status;

Enable Callid: Configure the caller number detection status;

Enable Reverse Polarity: Configure the polarity reverse status;

Dsp In/Out Volume: Configure the DSP volume. The negative means reducing and the positive means increasing.

Dtmf Silent: Configure the dialing interval;

Echo length: Configure the echo canceling time length;

Trunk code: Configure the trunk code;

Unit Code: Configure the unit code;

Scf: Configure the mute compression function. There are four options, that is, disable, mute packet SID, mute packet without SID, and mute packet PT13; disable means to disable the mute compression function; mute packet SID means sending SID frames; mute packet without SID means not sending SID frames; mute packet PT13 means sending SID frames and the SID frame type is indicated by 13.

Logical terminal type: Configure the logical terminal type. There are four options, that is, none, E1, FXO, and FXS. None means not to

configure; E1 means to configure as E1; FXO means to configure as FXO; FXS means to configure as FXS. The default value is none.

Jitter Buf: Configure the jitter buffer time length.

Dialtone Volume: Configure the dialing tone volume.

Enable DOD: Configure enabling the DOD function;

Enable Pulse Dial: Configure enabling the pulse dialing function;

FSK Msgtype: Configure FSK sending mode; there are two options, that is, sdmf and mdmf. The default value is sdmf.

Fsk Send Time: Configure the FSK sending time;

Fsk Start Time: Configure the FSK start time;

DOD parameter: To configure the DOD parameter, you need to enable the DOD function first;

Hot Line Number: Configure the hot line number;

Hot Line Wait Time: Configure the hotline wait time.

Configure the FXO port, as follows:

Figure 1-53 FXO port advanced configuration

Caution

The above is the FXO port advanced configuration of MyPower VGA600 and VG800.

Figure 1-54 FXO port advanced configuration

Caution

The above is the FXO port advanced configuration of MyPower VG2000.

Figure 1-55 FXO port advanced configuration

Caution

The above is the FXO port advanced configuration of MyPower VGM6000 and 6500.

Port: Display the voice port to be configured;

Enable: Configure port status;

Enable Callid: Configure the caller number detection status;

Enable Reverse Polarity: Configure the polarity reverse status;

Dsp In/Out Volume: Configure the DSP volume. The negative means reducing and the positive means increasing.

Dtmf Silent: Configure the dialing interval;

Echo length: Configure the echo canceling time length;

Trunk code: Configure the trunk code;

Unit Code: Configure the unit code;

Scf: Configure the mute compression function. There are four options, that is, disable, mute packet SID, mute packet without SID, and mute packet PT13; disable means to disable the mute compression function; mute packet SID means sending SID frames; mute packet without SID means not sending SID frames; mute packet PT13 means sending SID frames and the SID frame type is indicated by 13.

Logical terminal type: Configure the logical terminal type. There are four options, that is, none, E1, FXO, and FXS. None means not to configure; E1 means to configure as E1; FXO means to configure as FXO; FXS means to configure as FXS. The default value is none.

Jitter Buf: Configure the jitter buffer time length.

Dialtone Volume: Configure the dialing tone volume.

Busy tone: Configure the busy tone detection;

Dialtone type: Configure the dial tone type. There are three options, that is, {450Hz(the value:0)| 400Hz(the value:1)| 500Hz(the value:2)}

Enable Connection Plar: Configure the telephone number of the FXO port connection-plar. The call dialed in from FXO is directly forwarded to the connection-plar number, avoiding the secondary dialing process. The connection plar number can point to one specified FXS port of the gateway or the telephone number of the FXS, or the IVR access number of the gateway, or the other reachable number of the gateway route. The number dialed in from the FXO port is similar to the connection-plar number.

Enable FXS Linkage: Configure the FXS linkage function;

Wait dial tone: Configure the wait dial tone;

Wait Ring: Configure the ring delay;

FXO Plarout Configure: On the **FXO Plarout Configure** interface, you can set the caller number bound to the FXO port or one FXS port. Transfer Mode includes notrans and transfer if busy. When being configured as the notrans mode and the bound FXO port is unavailable, do not continue to search for other route any more and the call fails. When being configured as the transfer if busy and the bound FXO port is unavailable, continue to search for other available route. After FXO is bound with the caller number, the other number cannot call via the FXO port. Here, the bound caller number can carry the wildcard x, as follows:

Figure 1-56 FXO port caller binding

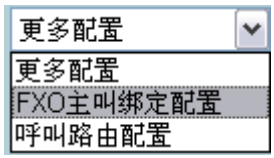
Caution

The above is the FXO port caller binding of MyPower VGA600M, VG800, and VG2000.

Caution

When selecting the check boxes before multiple ports, you can operate the ports in batches. If the selected are the different types of ports, display as follows:

Back: Return to the previous interface.

Select 

and enter the FXO caller binding configuration. The function is just for MyPower VGM6000 and VGM6500.

Figure 1-57 FXO caller binding

Caution

The above is the FXO caller binding of MyPower VGM6000 and 6500.

Click **Add**:

Figure 1-58 Add FXO caller binding

Port: Display the FXO port of the selected card;

Binding mode: You can select **Binding Number** or **Binding Port** (the binding port can only be the FXS type);

Transfer mode: Configure the transfer mode; there are two options, that is, notrans and transfer if busy.

Paging function: Vary with the displayed lines of each page. << means turning to the first page; < means turning to the previous page; > means turning to the next page; >> means turning to the last page. If there is only one page, do no change.

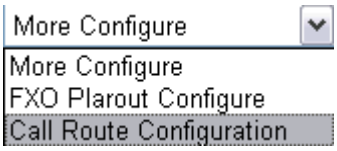
is used to delete one FXO caller binding configuration. After selecting the check boxes of the FXO caller binding configuration, click **Batch Delete** and you can delete the information of multiple FXO caller binding configurations.

Refresh: Refresh the current page.

Back: Return to the previous page.

Caution

When selecting the FXO caller binding configuration, the voice gateway needs to have the card with the FXO port. Otherwise, jumping fails. When displaying the configuration information, it also depends on the card. For example, card 2 only displays the information of the FXO caller binding configuration in card 2.



Select to jump to the call route configuration, which will be described in the call route configuration chapter.

Number Transform Configuration

Number transform is to transform the caller number of the user or the called number according to the pre-set rule. The called gateway performs the caller ID display according to the transformed caller number or the caller gateway routes according to the transformed called number. It is used for number plan. The dialing number can be different from the actual callout number. There are two kinds of transforming:

Caller number transform: Transform the caller number according to the pre-configured rule;

Called number transform: Transform the called number according to the pre-configured rule;

If the number transform rule is just configured on the gateway, but is not applied on one dialer, the rule does not take effect, that is, the number transform rule can take effect only after being bound with the dialer.

The number transform configuration interface includes the display of the configured number transform information and the number transform configuration, as follows:

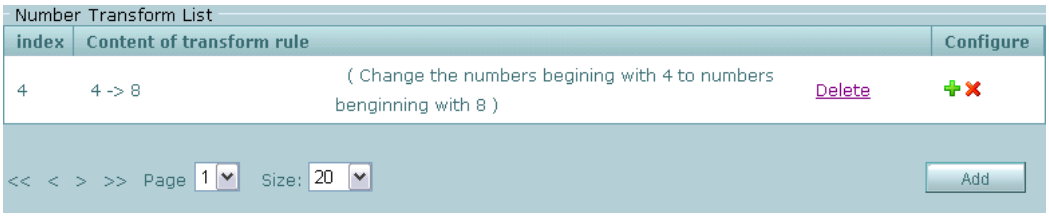


Figure 1-59 Number transform configuration

Click **Add** to display the following number transform configuration interface, as follows:

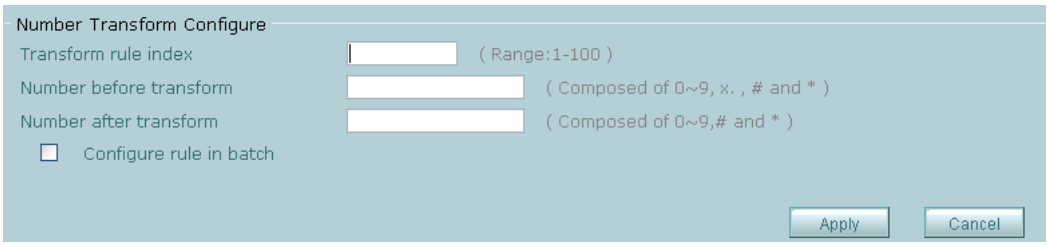


Figure 1-60 Add number transform

Number transform configuration include two modes. One is the configuration of one single rule. Click **Add** to enter the interface of configuring one single rule by default. The other is the configuration of batch rules.

As shown in the above figure, the configuration of one single rule includes three options, that is, transform rule index, number before transform and number after transform. Edit according to the rule prompted on the interface. After editing, click **OK** and you can see that the new number transform rule is already in the number transform configuration list; click **Cancel** to quit the input transform rule information. If the configuration rule is added by mistake or to delete the useless rule, you can click ✕ at the right of each line.

To configure the rules in batches, you can tick **Configure rule in batch** on the interface and the configuration area of the number transform is displayed as follows:

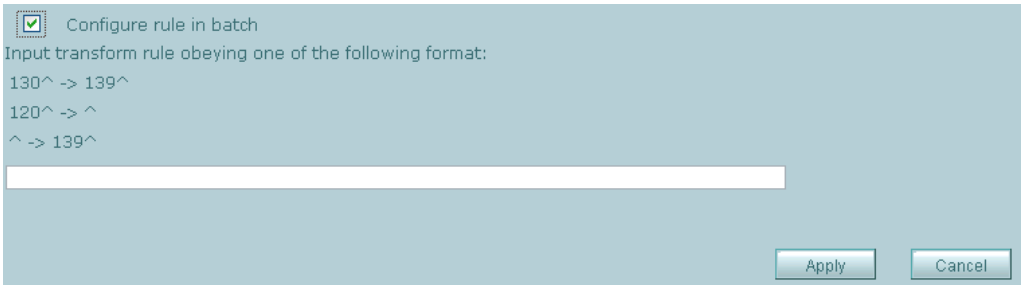


Figure 1-61 Batch number transform configuration

According to the rules prompted on the interface, edit the configuration options. After editing, click **OK** and the batch added transform rules are added to the list; click **Cancel** and you quit the input transform rule information. If some rule is added wrongly, you can click ✕ to delete it at the right of the list.

For example, if the number transform rule and call route have the following configuration:

The number transform configuration:

Figure 1-62 Number transform configuration

Call router configuration:

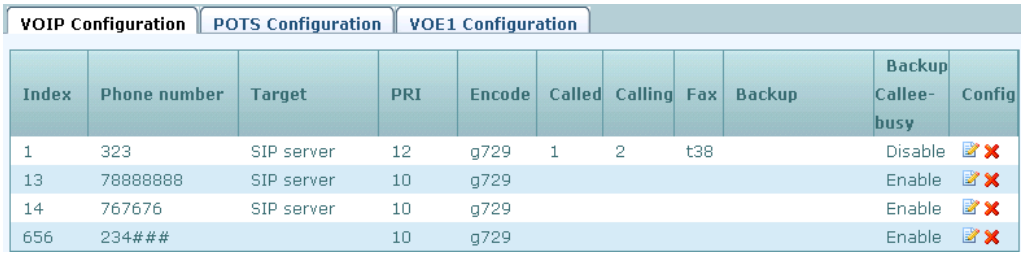


Figure 1-63 Call route configuration

Caution

The above is the call route configuration of MyPower VG2000 (with E1 card), VGM6000, and 6500.

The above figure indicates the call route with dialer as 1. When the caller number or called number begins with 3, change 3 to 5; if the caller number is 3456 and called number is 323, the seen caller number and called number on the called gateway are 5456 and 523.

Paging function: It changes with the displayed quantity. Click << and turn to the first page; click < and turn to the previous page; click > and turn to the next page; click >> and turn to the last page. If there is only one page, there is no change.

Call Route Configuration

Note

MyPower VG A600 and MyPower VG800 can configure VOIP and POTS routes, while MyPower VG2000 also can configure the VOE1 route besides the above two routes and the premise is that MyPower VG2000 is installed with the E1 card. MyPower VGM6000 and VGM6500 can configure all.

On the interface, you can view and edit the dialer route configuration, as follows:

Figure 1-64 Call route configuration

Caution

The above is the call route configuration of MyPower VGA600, VG800, and VG2000 (without E1).

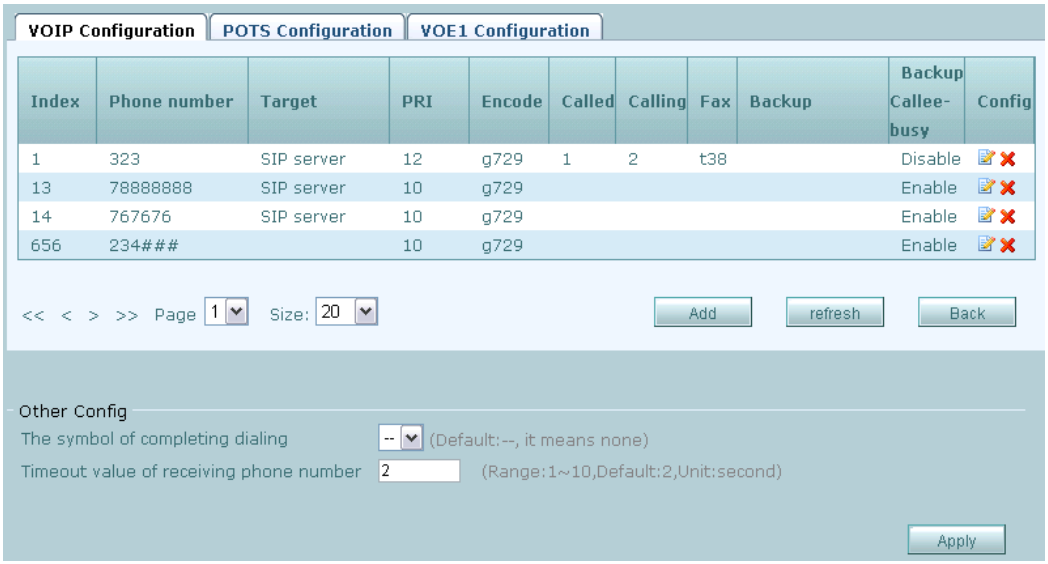


Figure 1-65 Call route configuration

Caution

The above is the call route configuration of MyPower VG2000(with E1 card), VGM6000, and 6500.

Click **VOIP Configuration or POTS Configuration** and you can perform the switchover of VOIP configuration and POTS configuration.

On the interface, you can view, edit and delete the information of the VOIP configuration and POTS configuration. VoIP corresponds with the remote IP phone or gateway via the IP network. POTS dialer configures the local call. After adding or modifying the telephone number, you need to re-register (when the gateway uses the H323 protocol, you need to re-register the gatekeeper; when the gateway uses the SIP protocol, you need to re-register the SIP server), which interrupts the ongoing calls. It is recommended to configure when the gateway does not make calls.

The symbol of completing dialing: After the user inputs the telephone number, input the symbol to end the inputting. Meanwhile, the gateway also quickly uses the call initiated by the received number. You can configure * or # as the symbol of completing dialing or do not configure it.

Timeout value of receiving phone number: The timeout of receiving the phone number; If the user does not have the dialing action during the time, the gateway automatically end receiving the number and uses the received number to initiate the call. The default value is 2s.

Click **Add** in **VOIP Configuration** to perform the VOIP configuration:

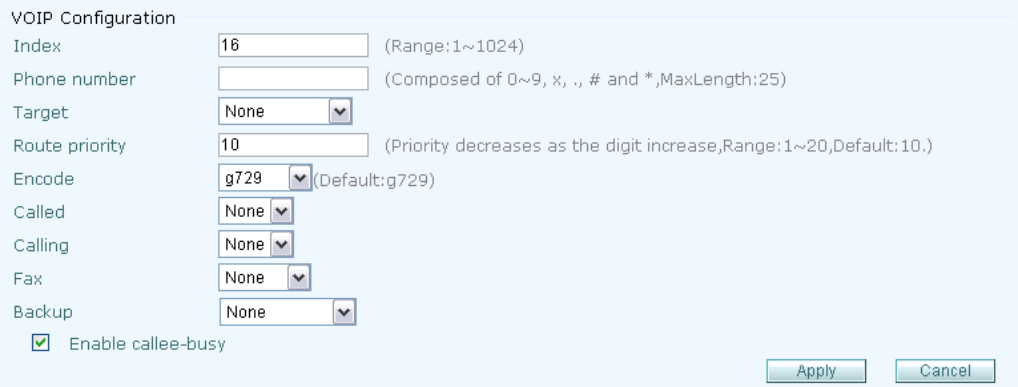


Figure 1-66 VOIP dialer configuration

Index: The serial number of the dialing rule;

Phone number: Configure the peer telephone number to be dialed;

Target: The peer gateway: Configure the IP address of the peer gateway (the address of the called gateway); gatekeeper: The destination address is gatekeeper; SIP server: the destination address is the SIP server;

Route priority: Configure the priority (1-20); the priority decreases when the number increases; the default value is 10; 20 means that the route is unavailable;

Encode: Configure the voice coding type first used by the IP call made by the dialing end;

Called: Use the number transition rule for the called number;

Calling: Use the number transition rule for the calling number;

Fax: Configure the fax function of the dialer. When the global fax protocol configuration conflicts with the fax protocol of the dialer, the fax protocol configuration of the dialer has higher priority.

When the global fax capability is configured as T.38:

If the fax capability of the dialer is configured as T.38: the current fax protocol is T.36;

If the fax capability of the dialer is configured as prohibit: there is no fax capability;

If the fax capability of the dialer is configured as transparent transmission: the current fax protocol is transparent transmission;

If the dialer is not configured as T.38: the current fax protocol is T.38;

When the global fax capability is not configured:

If the fax capability of the dialer is configured as T.38: the current fax protocol is T.38;

If the fax capability of the dialer is configured as prohibit: there is no fax capability;

If the fax capability of the dialer is configured as transparent transmission: the current fax protocol is transparent transmission;

If the dialer is not configured with the fax capability: there is no fax capability;

Caution

When the fax capability is prohibited in the dialer and if the call coding type is G.711, you can use the voice channel to transmit the fax data.

Backup: Configure the IPSWITCH function, realizing the IP-TO-PSTN or IP-TO-IP switchover after all IP links fail and ensuring that the call is re-routed from the secondary dialing end; switch to IP: switch to the other configured IP dialer and use the original called number to re-route; prefix: switch to the other configured IP dialer and add the prefix before the original called number as the new called number for re-routing; switch to PSTN: switch to the other configured PSTN dialer (contain POTS of the FXO port) and use the original called number for re-routing; prefix: switch to the other configured PSTN dialer (contain POTS of the FXO port) and add the prefix before the original called number as the new number for re-routing.

Enable callee-busy: Configure the route switching function when the called is busy;

SIP message carrying User Phone: Configure the SIP message to carry the User Phone parameter.

Click **Add** in **POTS Configuration** to perform the POTS configuration, as follows:

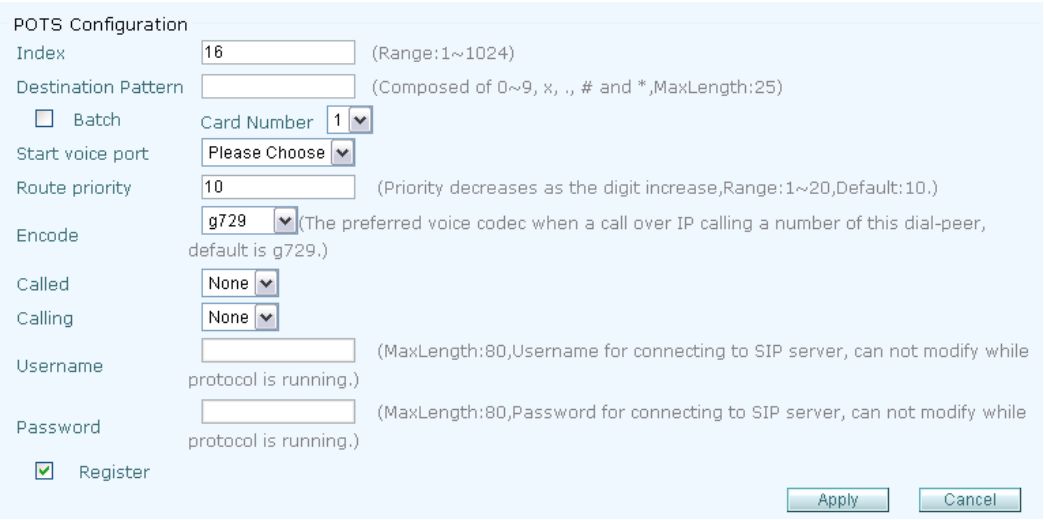


Figure 1-67 POTS dialer configuration

Index: The serial number of the dialing rule; the value range varies with the gateway dialer. For MyPower VG2000, VGM6000 and VGM6500, the value range is 1-1024; for VG800 and VGA600, the value range is 1-255.

Destination pattern: Configure the telephone number connected to FXS port; configure the dialing prefix from FXO to PSTN;

Batch: After selecting the Batch check box, you can perform the batch operation, as follows:

Figure 1-68 POTS batch port

Start/end voice port: Configure the POTS voice port; if the start voice port is the same as the end voice port, it is regarded to configure one single POTS dialing route; if different, it is regarded to configure the POTS dialing routes in batches. Each route corresponds to different voice port.

Number increase: If it is ticked, the telephone number automatically increases by 1 with the increasing of the port number;

Route priority: Configure the priority (1-20); the priority decreases when the number increases; the default value is 10; 20 means that the route is unavailable;

Encode: Configure the voice coding type first used by the IP call made by the dialing end;

Called: Use the number transition rule for the called number;

Calling: Use the number transition rule for the calling number;

Username: The user name connected to the SIP server; it is configured when using the SIP protocol;

Password: The password connected to the SIP server; it is configured when using the SIP protocol; the user name and password can be configured only when SIP is not registered to the server;

Register: Select whether to register to the gatekeeper or SIP server;

Hide Caller Number: Configure hiding the caller number.

Click **Add** in **VOE1 Configuration**:

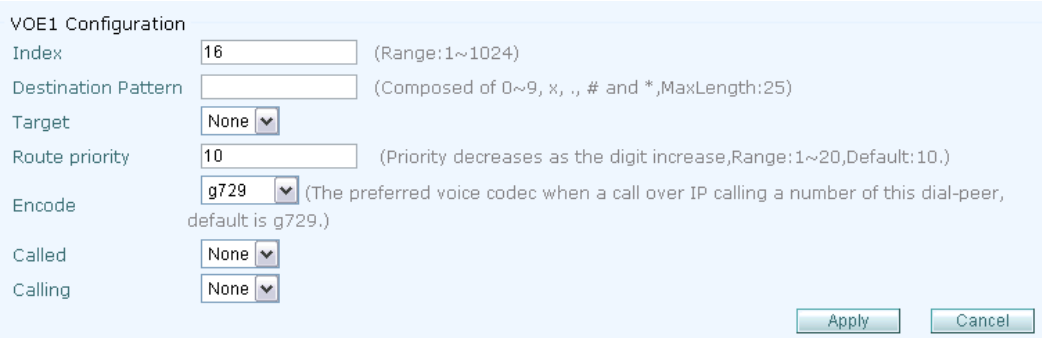


Figure 1-69 VOE1 dialer configuration

Index: The serial number of the dialing rule.

Destination pattern: The route number matching rule, including full number matching and prefix matching;

Target: Configure the voice port of the VOE1 side;

Route priority: Configure the priority (1-20); the priority decreases when the number increases; the default value is 10; 20 means that the route is unavailable;

Encode: Configure the voice coding type;

Called: Use the number transition rule for the called number;

Calling: Use the number transition rule for the calling number;

Black-white List Configuration

First, understand the black-white list model:

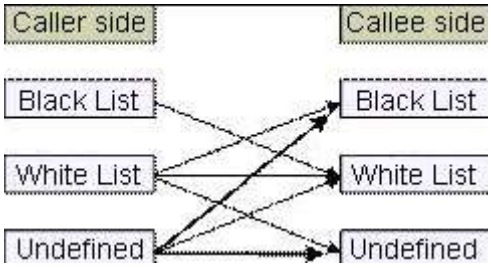


Figure 1-70 Black-white list model

The rules are shown below as arrows indicate:

The numbers in Calling Black List are feasible to call the numbers in the white list.

The numbers in Calling White List are feasible to call any called numbers.

The numbers in Calling Undefined is recognized as the numbers of the white list.

The **Black-white List Configuration** interface is shown as below: it is the configured black-white list bar with four buttons: **Add**, **Index conversion**, **Delete**, and **Refresh**.

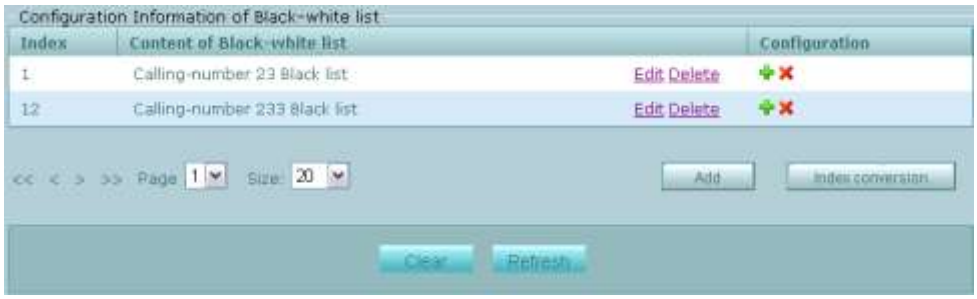


Figure 1-71 Black-white list configuration

Click **Add** and you can add new black-white list configuration. The contents to be edited are as follows:

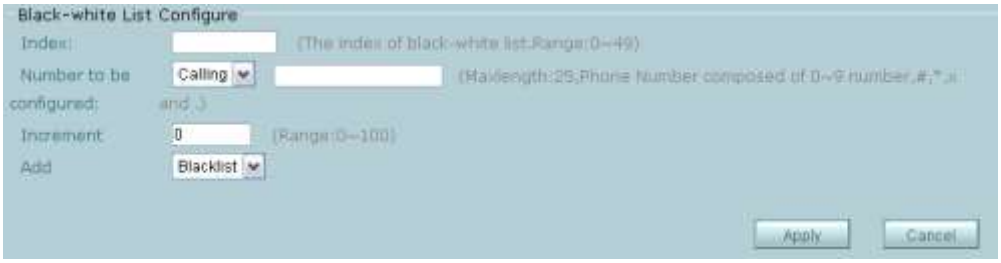


Figure 1-72 New black-white list

Index: The index of the black-white list. Range: 0-49

Number to be configured: number to be added in black-white list

Increment: The range of increment: 0-100

Add: add number to be configured to black list or white list (it can be the one with wildcard X.).

Click **Index Conversion** to change current index. The contents to be edited are as follows:

Figure 1-73 Index conversion of black-white list

Current Index: The source index of Black-white list index conversion.

Destination: The destination index of Black-white list index conversion.

Click **Clear** to clear the current black-white list configuration.

For example, if the black-white list has the following configuration:

Figure 1-74 Black-white list configuration

If calling number is 001 (in calling black list), it can be used to call called number 004(in called white list) only; if calling number is 002(in calling white list), it can be used to call any number; if calling number is 005(undefined in black-white list), it is recognized as white list number that can call any called number.

For called number not to be restrained, it is suggested that it should be added to called white list by default (namely, add called number xx. to

white list), or number in calling black list cannot call undefined called number.

The rule validity sequence of the black-white list is subjective to index, so calling number is matched with small index rule by priority. When the user matches one rule, don't try to match other rules. The user can adjust index order via index conversion. Under current sequence, the called number is 003 if calling number is 001. The rules with index as 1 are all valid in black-white list inquiry. At this time, call building is disabled for calling number and called number are all contained in black list. Make index conversion:

Figure 1-75 Conversion index

Index sequence changes like this:

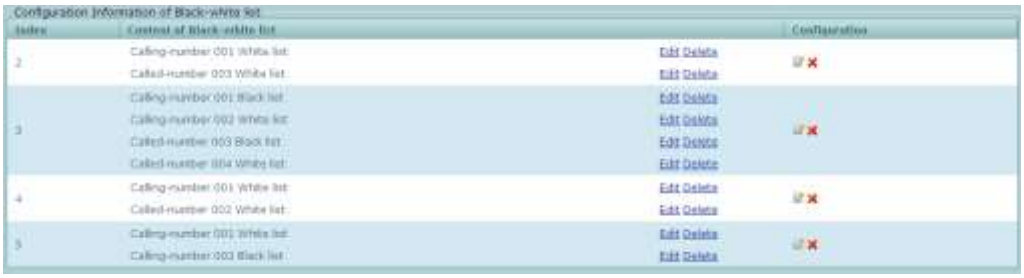


Figure 1-76 Black-white list configuration

Adjust the original rules with index as 1 to the position of rules with index as 3, and then shift back rules with index as 3 and other rules in sequence.

In current sequence, the called number is 003 if the calling number is 001. In black-white list matching, the rules with index as 2 are valid. At this time, call building is enabled for calling number and called number are all contained in white list.

Call Service Configuration

On this interface, the user can configure call service configuration services, including Enable/Disable call transfer service, call divert service and call wait service.

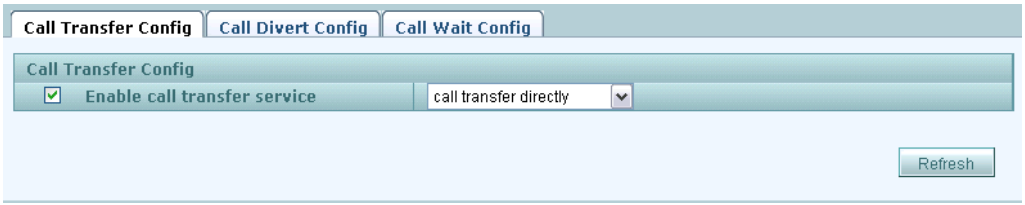


Figure 1-77 Call transfer service configuration

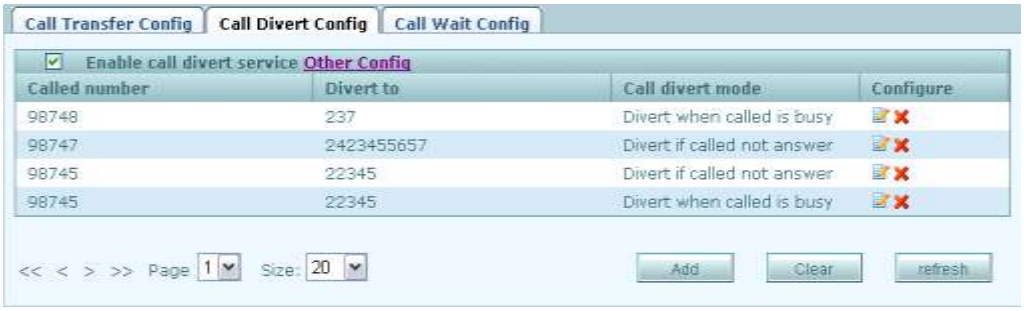


Figure 1-78 Call divert service configuration

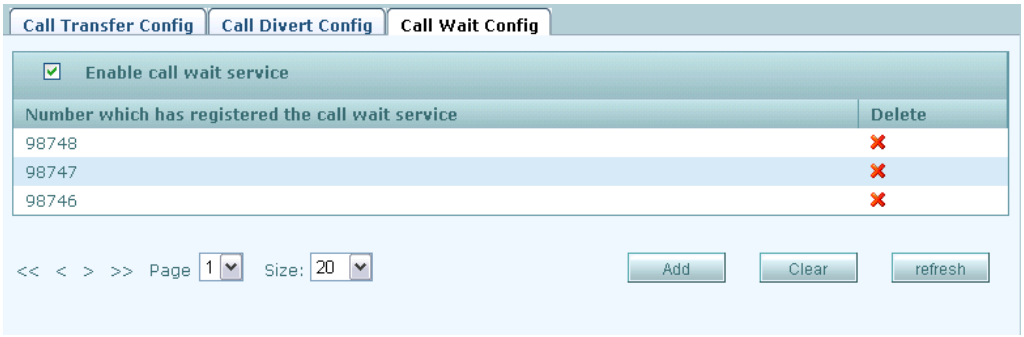


Figure 1-79 Call wait service configuration

Click **Call Divert Config** or **Call Wait Config** to perform the switch between call divert service and call wait service.

Call transfer configuration:

User A is the one that has right to use call transfer service. During communication between user A(called user)and user B(calling user), user A can transfer current calling between A and B to new calling between user B and user C. User C plays a role as the one to be transferred. Once call transfer is completed, user B and user C can communicate with each other, while user A will no longer communicate with user B or user C.

Click **Enable call transfer** to start call transfer service. It is enabled only if the gateways of A and B both enables the configuration.

Call transfer includes direct transfer and call transfer after inquiry. During the direct transfer, user A does not communicate with user C, and the communication between user A and user B is transferred to the communication between user B and user C. During all transfer dafter inquiry, after contacting user C, user A recognizes that user C can better

solve problems of user B, and then it is transferred to the communication between user B and user C.

For details, refer to the related chapter of MyPowerVG Gateway Configuration Manual V8.0.

Caution

Call transfer supports caller transfer and callee transfer.

Call divert configuration:

Click **Other Config** in **Call Divert Configuration** to configure the no answer expiry time before transfer:

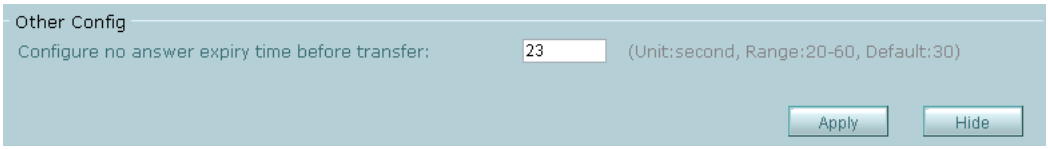


Figure 1-80 Other configuration

Click **Enable call divert service** checkbox to start call divert service.

Click **Add** to add a call divert service: Click the Edit icon and you can edit the current information.

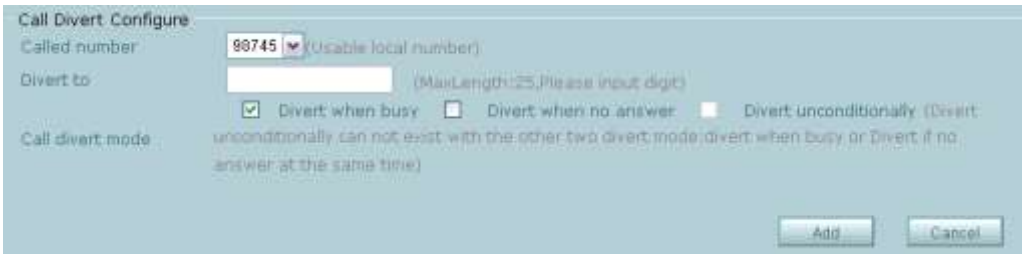


Figure 1-81 New call divert

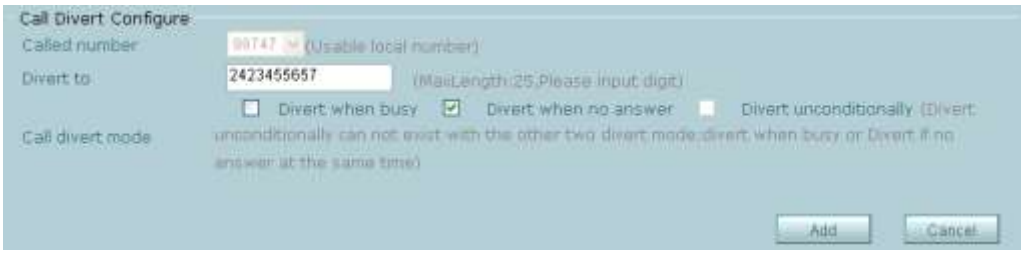


Figure 1-82 Edit call divert

Called number: choose a feasible local number

Divert to: the number divert to. The route number match rule includes complete number match or prefix match.

Call divert mode: configure divert conditions.

The application of Call Divert:

1. Call divert takes effect automatically after configuration rather than manual application.
2. When the calling and the called are not in the same gateway, divert will not succeed only if the calling user supports H450.3 or Q.931 Facility call forwarding mode when using H.323 protocol, or supports SIP protocol standard divert procedure when using SIP protocol. For call divert based on H323 protocol or SIP protocol, the calling gateway can perform calling without call route configuration if the message received by the calling gateway contains IP address of user diverted. Otherwise, call route configuration is necessary.

Caution

For divert refers to several diverts in complicated network environment, the fault is displayed by busy tone directly in common divert.

Introduction to call waiting:

Call Waiting informs the user of new call for user to accept, reject or leave it unanswered. For example, user A is communicating with user B that has registered call waiting service. At the same time, user C tries to call busy B. The Router will send user B a prompt, namely, 'beep, beep, beep' tone, which indicates a call waiting. User B can choose to accept, reject or leave it unanswered

If user B does not make choice during call waiting, the user C hears the call waiting tone.

Call Wait Configuration:

Click the **Enable call wait** checkbox in **Call Wait configuration** to initiate call wait service.

Click **Add** to add a new wait service:

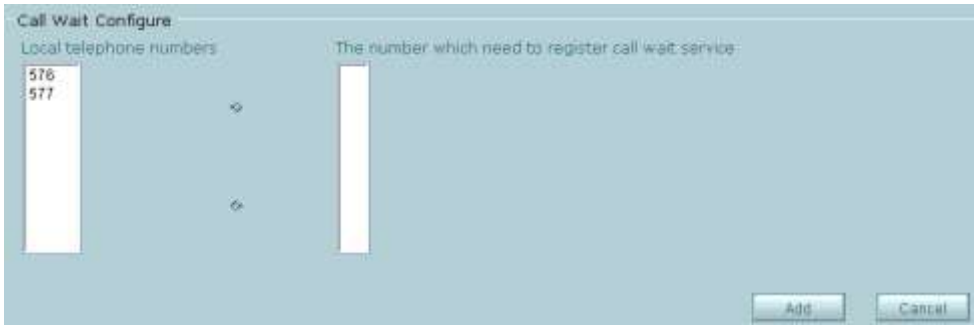


Figure 1-83 New call wait

Choose a telephone number from **Local telephone numbers** and press to add it to **the number which need to register call wait service**. Finally, press **Apply** to set it as the number which needs to register call wait service. Press to delete the chosen number from '**The number which need to register call wait service**'.

Caution

The voice port of the local number used by the service should be enabled and the number does not register other call service. The system filters the local numbers registering other call service and the disabled voice port is also filtered automatically.

The application of Call Wait:

Follow the instructions below to choose, reject or leave unanswered the new call:

Press hook-switch and then press '1' to reject new call.

Press hook-switch and then press '2' to receive new call.

No action indicates to leave it unanswered.

After receiving new call, the user can switch between two communications at any time. Follow the steps below:

Press hook-switch and then press '2' to switch between the new users and the old users.

Note

If a number is configured with the Call Divert service, first delete it from the Call Divert service and then you can configure Call Wait service. If a number is configured with the Call Wait service first, you do not need to

delete the Call Wait service before configuring the Call Divert service. The gateway can use Call Divert service first according to the service priority.

Call Pickup Configuration

Call pickup means that when the phone of the called user A rings, user B hopes to answer the call of user A by performing some operation on its own phone; when user B answers the call, the phone of user A stops ringing. The gateway can configure call pickup group. The dialing mode for call pickup of users in the group is different from that of the users that are not in the group.

1. User A and user B belong to a call pickup group. User B picks up the phone and dials *71*# or dialing*71* times out, that is, user B does not need to dial the phone number of user A to answer the call of user A.

2. User A and User B do not belong to a call pickup group. User B picks up the phone and dials *71* the phone number of user A # or dialing *71* the phone number of user A times out.

Note

In the above two points, if you want to use # to end the dialing, you need to configure the ending symbol of receiving number on the Call route configuration interface as #. If you do not want to use #, the gateway waits for the timeout of receiving number. The gateway performs the call pickup operation according to the received number.

By default, the gateway enables the call pickup function that is not in the group, but if you want to perform the call pickup in the group, you need to do the corresponding configuration. In a call pickup group, you can only configure the FXS port.

The call pickup configuration interface is as shown in the following figure. On the interface, you can add, edit and delete the call pickup group.

Figure 1-84 Call pickup configuration

Note

1. One device allows to be configured with up to 10 call pickup groups.

2. Only the FXS port of the device can be configured with the port of the call pickup group.

3. The call pickup group does not allow the number of the ports as 0. When adding a call pickup group, you need to add at least one port. Otherwise, adding a call pickup group fails. Contrarily, if you delete the last valid port in the call pickup group, the call pickup group is deleted at the same time.

Click **Add Group** to enter the following configuration interface. Input the information of the new call pickup group on the interface, and click **Set**. Click **Back** to return to the interface of displaying call pickup groups.

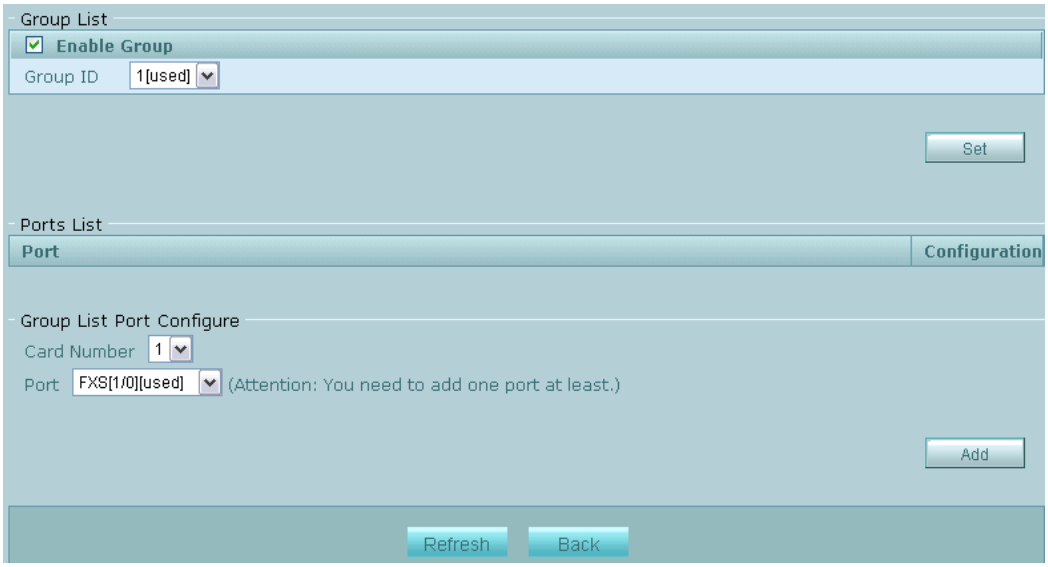


Figure 1-85 New call pickup

Enable Group: Enable/disable call pickup group. Tick **Enable Group** check box to enable call pickup group.

Group ID: The serial number of the call pickup group. The value range is 1-10.

Port: Configure the port of the call pickup group.

Group Ring Configuration

Group ring is one service of local gateway FXS/FXO card. When there is incoming call and if the called number matches the number of the group ring, the phones of all FXS ports in the group ring at the same time. The FXO in the group initiates the call to the corresponding configured number via the port. But as long as one port is connected, the other ports stop ringing and recover the original status.

The group ring configuration interface is as shown in the following figure. On the interface, you can add, edit and delete the ring group.

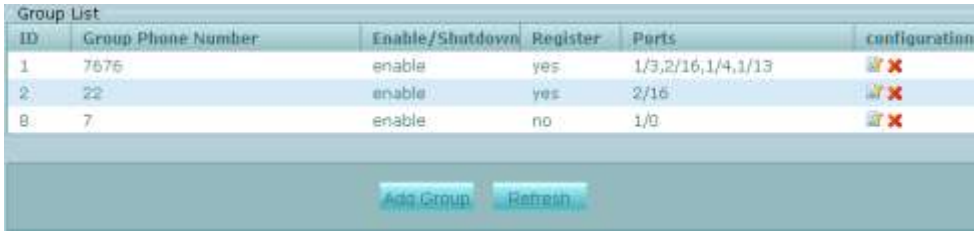


Figure 1-86 Group ring configuration

Note

1. One device can be configured with up to 50 ring groups.

2. The FXS and FXO ports of the device allow to be configured as the ports of the ring group. When configuring FXO port, you should specify the corresponding phone number.

3. If the group contains the FXO port, the external line connected to the FXO port needs to provide the reverse polarity signals and the FXO port needs to Enable the configuration of checking reverse polarity signals.

Click **Add Group** to enter the following configuration interface. Input the information of the new ring group on the interface, and click **Set**.

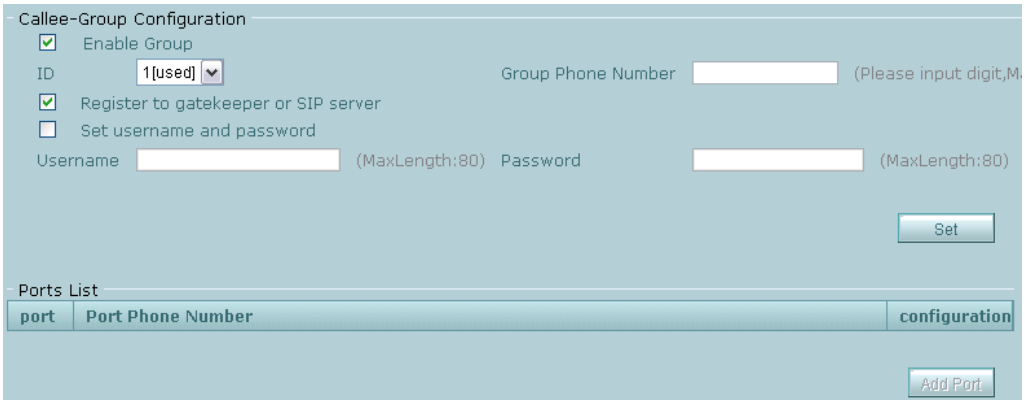


Figure 1-87 Add group ring

Enable Group: Enable/disable the ring group.

ID: The serial number of the ring group.

Group Phone Number: The group ring number matched with the called number.

Register to gatekeeper or SIP server: Enable/disable group ring number register to SIP register server or gatekeeper. By default, it is enabled.

Set username and password: Whether to configure the user name and password of the group number for registering SIP server. The username and password can be configured only when the SIP protocol is not in the register state.

Username and password: The username and password of the group number, used for registering SIP server.

Port: The port of the group ring.

The **Add Port** button is in the active state only after the group ring is added successfully or editing the existing group ring. Click it to enter the following port configuration interface. On the interface, you can select the member ports to be added to the ring group. If FXO port is selected, the phone number of the FXO port should be configured. One ring group can be configured with up to two member ports.

Figure 1-88 Add port

IVR System Configuration

IVR (Interactive Voice Response) user can realize second dial-up by dialing called number according to the tone after dialing a number to gateway. IVR system configuration includes IVR basic configuration and VR play option configuration.

IVR configuration interface is shown below:

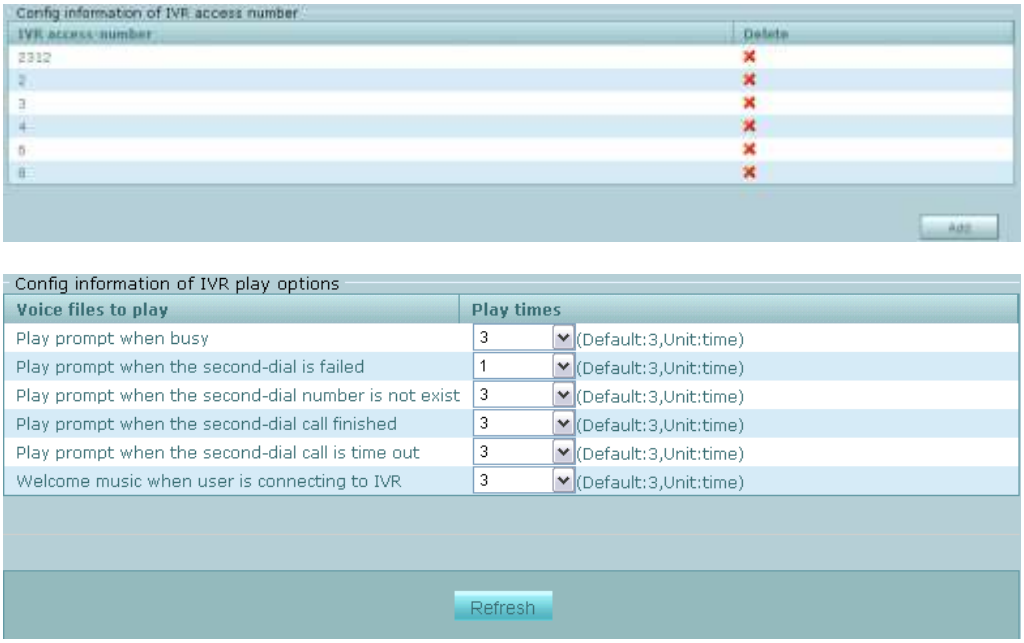


Figure 1-90 IVR basic configuration

Enable IVR: Tick the Enable IVR check box. Otherwise, disable the IVR service.

IVR record number: Configure the IVR record number. After the user dials the IVR access number, dial the IVR record number. After hearing the prompt tone, press * to begin recording. Press # or hang up to end the recording. The recorded file is restricted by the IVR record time and code. Null means not to configure.

IVR Record Time: Range: 5-60, Default: 60.

IVR record codec: There are three codes, including G.729, G.723 and G.711. The default value is G.729.

Register IVR access numbers to gatekeeper or SIP server: After ticking the item, the IVR access number is registered to the gatekeeper or SIP server. Otherwise, do not register.

Enable IVR authentication: when IVR authentication is enabled, the system requires the user to input username and password during access number dialing. The user is able to use IVR service only if he gets successful authentication in server. (For this function, it should be in accordance with Maipu NetSmart server. At the same time, the user should configure AAA authentication in gateway.)

IVR access number: You can configure multiple IVR access numbers. The IVR access number comprises numbers with a length of 1-25 digits. Null means not to configure. Click **Add** and you can configure more IVR access numbers.

Figure 1-91 IVR access number configuration

As the figure illustrates, the left are the voice files to play, while the right are play times of voice files. The user should choose one proper parameter according to requirements from four types: 1, 2, 3 or cycle.

For details, refer to the related chapter of MyPowerVG Gateway Configuration Manual V7.0.

Caution

1. When the called hangs up or cannot be connected, the caller can continue to dial other extension for five times at most;

2. When the IVR authentication function is enabled, the AAA authentication function also needs to be configured. The user name and password can be input wrongly for three times at most. After three times, you directly hear the busy tone.

Accounting Authentication Configuration

The accounting authentication server matched with Maipu voice gateway is NetSmart accounting authentication server. If you want to account or authenticate the calls of the gateway, install NetSmart accounting authentication server on a PC in the network and Set IP address of the PC on the VoIP gateway as Radius server address. The following is the configuration interface of NetSmart accounting authentication.

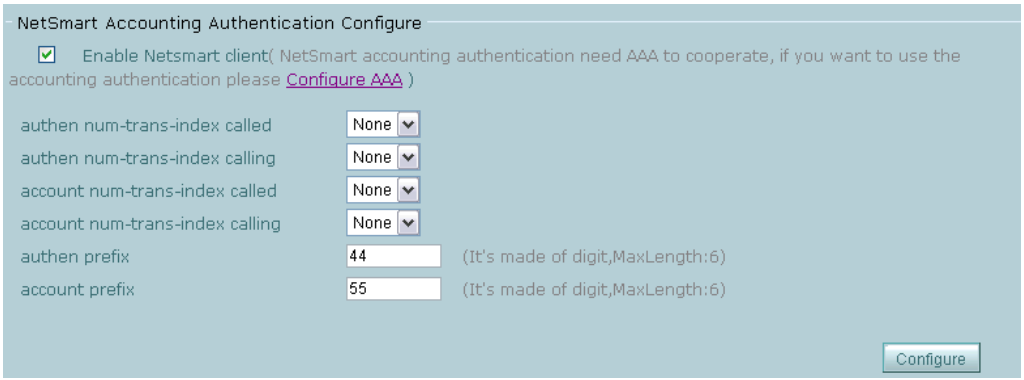


Figure 1-92 Accounting authentication configuration

authen num-trans-index calling: Configure the called number transform rule of the authentication;

authen num-trans-index called: Configure the calling number transform rule of the authentication;

account num-trans-index calling: Configure the called number transform rule of the accounting;

account num-trans-index called: Configure the calling number transform rule of the accounting;

authen prefix: Configure the authentication prefix of the device;

account prefix: Configure the accounting prefix of the device;

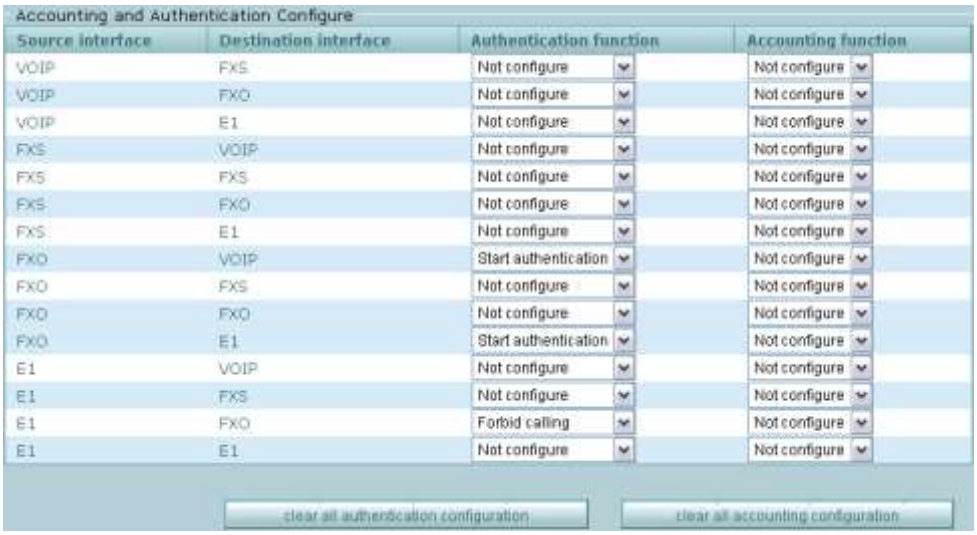


Figure 1-93 Accounting authentication configuration

Caution

The above figure is the accounting authentication configuration of MyPower VG2000 (with E1), VGM6000, and 6500.

Figure 1-94 Accounting authentication configuration

Caution

The above figure is the accounting authentication configuration of MyPower VG2000 (without E1), VGA600, and VG800.

The accounting needs the cooperation of AAA, so you need to configure AAA first before enabling the accounting authentication. The AAA configuration interface is as follows:

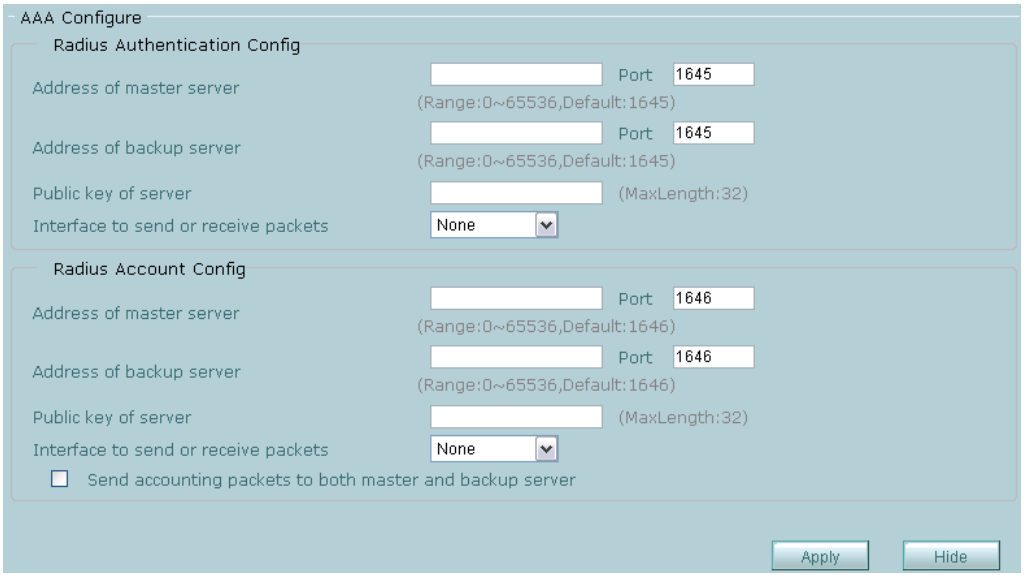


Figure 1-95 AAA configuration

Radius authentication server configuration:

Address of master server: The IP address of the preferred Radius protocol authentication server of the voice gateway;

Address of backup server: When the Radius master server cannot be used, adopt the standby server to authenticate;

Port: The communication port of the gateway and Radius accounting server; the default value is 1645;

Public key of server: One key shared by the network access server (that is NAS; usually, it is one gateway, such as VG2000 gateway) and Radius authentication server. The shared key of the Radius server is configured in the NAS configuration on the Radius server. The authentication can be performed only when the shared key of the network access server and Radius authentication server.

Interface to send and receive packets: The network communication interface used by the authentication message transmission between the gateway and Radius authentication server.

Radius account config:

Address of master server: The IP address of the preferred Radius accounting server of the voice gateway;

Address of backup server: When the Radius master server cannot be used, adopt the standby server to account;

Port: The communication port of the gateway and Radius accounting server; the default value is 1646;

Public key of server: One key shared by the network access server (that is NAS; usually, it is one gateway, such as VG2000 gateway) and Radius authentication server. The shared key of the Radius server is configured in the NAS configuration on the Radius server. The accounting can be performed only when the shared key of the network access server and Radius accounting server.

Interface to send and receive packets: The network communication interface used by the authentication message transmission between the gateway and Radius accounting server.

Send accounting packets to both master and backup server: If this item is ticked, send the accounting packets to the master and backup servers.

The source port type and destination port type of the communication are fixed. What the user needs to do is configuring each type of authentication function and accounting.

The authentication function includes enable authentication, not configure and prohibit call:

Enable authentication: The communication between the source port and the destination port needs to be authenticated by the Radius protocol accounting authentication server (or other protocol authentication server). The communication can be performed only the authentication succeeds. Otherwise, the communication is not permitted.

Not configure: Do not be authenticated by the authentication accounting server. The communication between the source port and the destination port is permitted;

Forbid calling: Prohibit the call between the source port and the destination port;

The accounting function has two types: Configure or Not Configure.

Configure: perform accounting for the communication between source interface and destination interface.

Not Configure: not to perform accounting for the communication between source interface and destination interface.

The user can configure authentication accounting option for ports according to specific requirements. There is no configuration option for authentication accounting configuration for communication from VOIP to VOIP.

Click **Clear all authentication configurations**, and not configure is set automatically for authentication Function.

Click **Clear all accounting configurations**, and not configure is set automatically for accounting Function.

Fax Service Configuration

Currently, support two fax modes, that is, T38 fax mode and transparent transmission mode. The T38 fax mode includes the UDPTL mode and RTP mode.

The configuration interface of the fax service is as follows:

Figure 1-96 Fax service configuration

Caution

The above figure is the fax service configuration of MyPower VGM6000 and 6500.

Figure 1-97 Fax service configuration

Caution

The above figure is the fax service configuration of MyPower VG800 and VG2000.

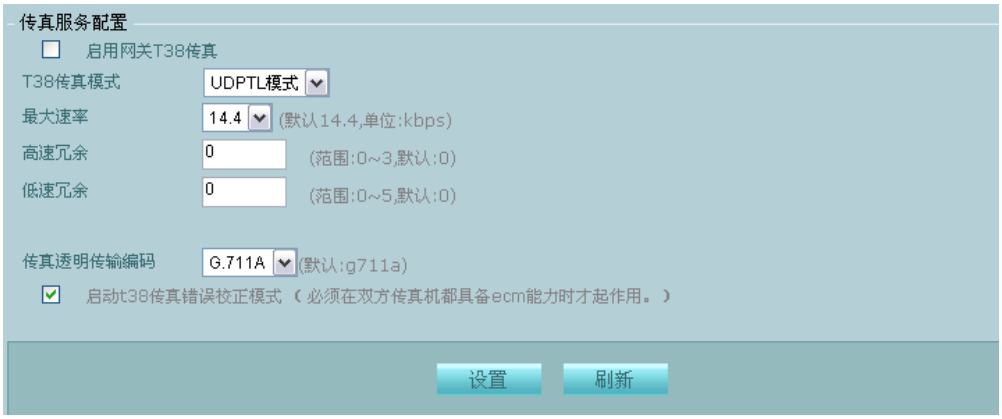


Figure 1-98 Fax service configuration

Caution

The above figure is the fax service configuration of MyPower VGA600.

Enable global T.38 capability of this gateway: To enable T.38 capability of the gateway aims at the global gateway. Once T38 capability configuration is started, the global gateway supports T38 fax capability, or the user can configure T38 fax capability under some dial port or disable T38 capability for some dial port. When the gateway is configured as the caller, it decides whether to support T38 fax by detecting backwards according to the calling number. Attention: it is feasible under VOIP dial port only.

🕮 **Note**

The user can configure fax capability under VOIP port only. It is invalid under other dial ports. Only if the gateway is configured with enable gateway T38 fax and VOIP dial port has corresponding fax capability (such as T38 or transparent fax), the gateway gives the priority to fax capability under dial port.

T38 fax mode: On the premise of T38 capability, the encapsulation mode of T38 ASN.1 IFP packet includes UDPTL mode and RTP mode. The payload type used by the RTP fax mode is 98. The payload type used by RTP fax mode cannot be the same as the dynamic payload type used by 2833 protocol.

Maximal Speed: Unit: kbps, default: 14.4kbps. The fax speed is used to control maximal speed of fax, that is, the fax negotiates from the configured maximum speed.

High Redundancy: It is the number of the redundant packets in T38 high-speed data. When the fax is seriously distorted, it is the times of re-transmitting fax packets. The fax quality can be improved by increasing the value when the network is in the bad state and there is packet loss.

Low Redundancy: It is the number of the redundant packets in T38 low-speed data. When the fax is cannot be connected, it is the times of re-transmitting T38 connection messages. The fax quality can be improved by increasing the value when the network is in the bad state and there is packet loss.

Fax transparently transmitting codes: To support the encryption fax, you need to use the transparent transmission mode. During the transparent transmission, the gateway does not understand the fax signaling and data, but encapsulates in the lossless compression coding mode and transmits to the peer gateway transparently. The gateway supports three kinds of lossless compression coding modes, that is, G.711A, G.711U and G.726. The transparent transmission requires that the coding types of the two gateways are consistent.

Adjust fax code mode: After enabling the command, modify the voice code to the PCMA code before starting fax.

Enable Error Check Mode of T38 fax: It takes effect only when the electrographs of the two sides have the ECM function.

Adjust the volume of fax: Configure the fax volume when the fax signal tone is abnormal and the fax cannot succeed.

Other Configurations

The following figure illustrates other VoIP service configurations:

Figure 1-99 Other configuration

Caution

The above figure shows the other configuration of MyPower VGM6000 and 6500.

Figure 1-100 Other configuration

Caution

The above figure shows the other configuration of MyPower VGA600, VG800, and VG2000.

Code mode that this gateway supports: To meet the using requirements of different users, the low-end gateway (MyPower VG2000, VG800, and VG A600) supports two coding modes. Different coding modes use different codes.

FSK mode: There are two modes, that is, v23-mode and bell202-mode, whose mark (1) and space (0) frequency are different.

DTMF signal gain: Do not change this if not necessary (e.g.: DTMF signals sent from FXO port cannot be identified by exterior port because of too low volume).

Voice Data TOS: There are two modes: preference sending mode and normal sending mode. To improve sending performance of IP voice packet in IP network, set TOS field of IP head in a higher priority level in IP package via preference sending mode. Thus, system will give priority to IP data processing in network sending as long as IP transfer points in IP voice packet access support IP TOS prosperity.

Area Code: If the calling number starts with a header as the same as this code, the header is discarded before displaying onto the FXS.

FXO external line detection time: Configure the interval of FXO external line detection. The default value is 10 minutes. By default, the FXO external line detection function is enabled and the configuration is null, which means to disable the external line detection function. The external line regularly checks whether the FXO port is connected with the phone cable. If yes, the call route transfers the calls to the FXO port; if no, the call route does not transfer the call to the FXO port.

FXS Ring Delay: Configure the FXS ring delay.

FXO Dial-out Flash hook Time: configure FXO dial-out flash hook time. Set a larger value for bad connection in FXO dial-out.

Configure Echo Cancellation: There are two options, that is, 25ms and 40ms. The default value is 25ms. Only MyPower VG2000 has the configuration.

Check UDP Checksum: whether perform UDP check on voice packet and fax packet in IP calling.

Play Ring back to Caller: enable or disable ring back function of gateway in IP calling.

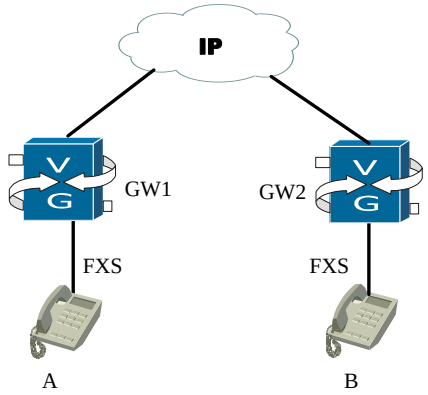


Figure 1-101 Play ring-back tone

Assume that A is calling user and B is called user. GW1 of user A (A can be other terminals such as IAD which is connected via soft-switch) cannot play ring back to A.

When user A calls B, B is ringing. Assume that GW2 starts FXS remote ring back function, when GW2 rings B, it sends similar ring back tone to user A after connecting AB medium access via the negotiation with GW1. In such case, user A can hear ring back tone.

Individual ring: Whether to enable individual ring function. After enabling the function, the gateway distinguishes the IP calls and non-IP calls via ring modes. By default, the function is disabled.

IP callout indicate: Whether to Enable IP callout prompt. By default, it is disabled. When it is enabled, there are two parameters: IP callout indicate interval and continue:

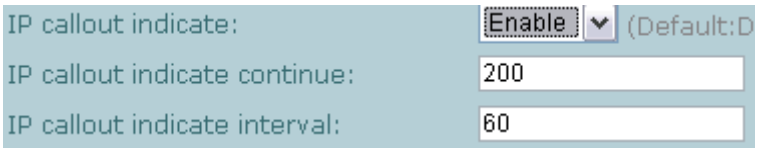


Figure 1-102 IP callout prompt tone

IP callout indicate continue: The unit is ms; value range is 100-500; the default value is 200.

IP callout indicate interval: The unit is ms; value range is 30-120; the default value is 60.

Total IP call: IP calls include incoming IP call and outgoing IP calls. 0 means prohibiting IP calls.

Playing music when the third party is held: After enabling the function, the local gateway plays music to the held party after the gateway phone receives the holding signals. Otherwise, the remote gateway or soft terminal plays the music.

System prompt language type: Currently, English and Chinese voice prompts are provided. By default, it is Chinese. Before selecting the language type, please confirm whether the corresponding voice file is downloaded to the gateway FLASH. If not, please download it. Otherwise, it cannot be played after configuration.

Voice Vlan: Enable or disable the Voice Vlan function; when the Voice Vlan function is enabled, Vlan Id should be configured.

Vlan Id: Configure Vlan Id.

FXS global configuration: Configure the global attributes of all FXS cards of the gateway. There are the following three configuration items:

Dial interval: The value range is 10-100; the unit is 10ms; the default value is 30;

Flash-hook length lower limit: The value range is 4-100; the unit is 10ms; the default value is 13.

Flash-hook length upper limit: The value range is 4-100; the unit is 10ms; the default value is 60.

Simulative Call Test

The simulative call test of the voice service configuration is as follows:

Figure 1-103 Simulative Call Test

Calling number: The calling number in the simulation test.

Called number: The called number in the simulation test. It is mandatory.

After inputting the desired number, click **Start Test** and the status varies with the returned information in the device, as follows:

Figure 1-104 Simulation call test

To stop the test, click **Stop Test**.

Voice Call Port Status

The voice call port status of the voice service configuration is as follows:

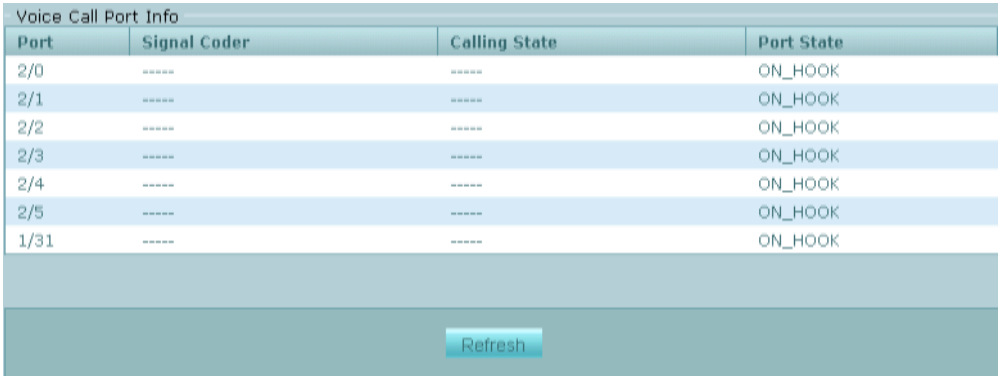


Figure 1-105 Voice call port status

Current Call Communication Statistics

The current call communication statistics of the voice service configuration is as follows:

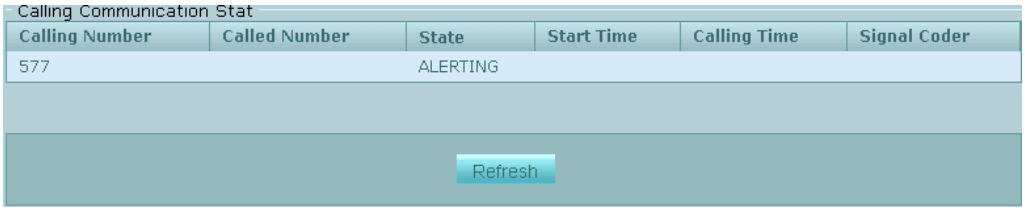


Figure 1-106 Current call communication statistics

CSC Card Configuration

The CSC card configuration is as shown in the following figure. Currently, only 6000 and 6500 support the function.

Figure 1-107 CSC card configuration information

Click **Add**:

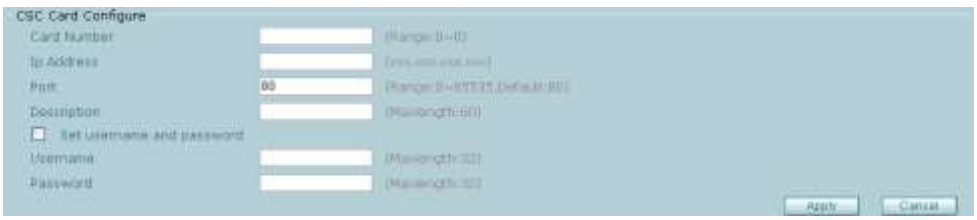


Figure 1-108 Add CSC card configuration

Click **Edit**:

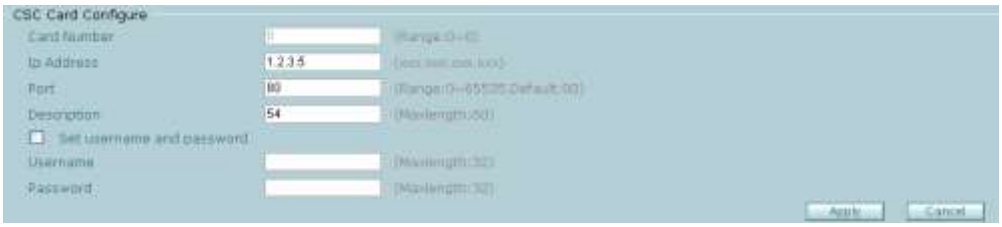


Figure 1-109 Edit CSC card

Card Number: The value ranges of 6000 and 6500 are different. 6000 only supports 0 and 6500 supports 0-6.

Ip Address: Configure the IP address.

Port: Configure the port number.

Description: Configure the description information.

Set username and password: Enable or disable the configuration of the user name and password.

Username: Configure the user name.

Password: Configure the password.

Click ✖ to delete the corresponding CSC card configuration information.

MTP/TUP Timer Configuration

The MTP/TUP timer configuration includes MTP2 timer configuration, MTP3 timer configuration and TUP timer configuration.

Figure 1-110 MTP2 timer configuration

MTP2 定时器 | MTP3 定时器 | TUP 定时器

MTP3 定时器配置

定时器名称	配置		描述
MTP3 T1	80	(范围：50~120, *10ms 默认：80)	避免消息倒换后消息发生顺序错误的延时
MTP3 T2	140	(范围：70~200, *10ms 默认：140)	等待倒换证实
MTP3 T3	80	(范围：50~120, *10ms 默认：80)	时间受控传递-避免倒回后顺序错误的延时
MTP3 T4	80	(范围：40~120, *10ms 默认：80)	等待倒回证实（第一次尝试）
MTP3 T5	80	(范围：40~120, *10ms 默认：80)	等待倒回证实（第二次尝试）
MTP3 T6	50	(范围：40~120, *10ms 默认：50)	避免受控重选路由后，消息顺序错误的延时
MTP3 T7	100	(范围：100~200, *10ms 默认：100)	等待信令数据链路连接证实
MTP3 T8	80	(范围：80~120, *10ms 默认：80)	禁止传递的抑制定时器
MTP3 T10	800	(范围：800~6000, *10ms 默认：800)	等待重发信号路由组测试消息
MTP3 T11	3000	(范围：3000~6000, *10ms 默认：3000)	受限传递定时器
MTP3 T12	100	(范围：80~150, *10ms 默认：100)	等待解除阻断证实
MTP3 T13	100	(范围：80~150, *10ms 默认：100)	等待强制解除阻断
MTP3 T14	250	(范围：200~300, *10ms 默认：250)	等待阻断证实
MTP3 T15	200	(范围：200~300, *10ms 默认：200)	等待启动信令路由组拥塞测试
MTP3 T16	140	(范围：140~200, *10ms 默认：140)	等待路由组拥塞状态修改
MTP3 T17	100	(范围：80~150, *10ms 默认：100)	为避免初始定位故障和链路重新启动来回的延时
MTP3 T22	600	(范围：300~600, *10ms 默认：600)	本地阻断测试定时器
MTP3 T23	600	(范围：300~600, *10ms 默认：600)	远端阻断测试定时器

刷新 提交

Figure 1-111 MTP3 timer configuration

MTP / TUP 定时器配置

MTP2 定时器 | MTP3 定时器 | TUP 定时器

TUP 定时器配置

定时器名称	配置		描述
TUP T1	15	(范围：10~15 sec 默认：15)	等待接续或接续失败信号定时器
TUP T2	30	(范围：20~30 sec 默认：30)	等待地址全消息定时器
TUP T3	15	(范围：4~15 sec 默认：15)	发送不成功消息后，等待前向拆线信号定时器
TUP T4	15	(范围：4~15 sec 默认：15)	发出呼叫失败信号后，等待前向拆线信号定时器
TUP T6	15	(范围：4~15 sec 默认：15)	等待释放监护信号定时器
TUP T9	10	(范围：1~10 sec 默认：10)	启动第一次导通校验时延定时器
TUP T10	180	(范围：60~180 sec 默认：180)	多次重复导通检验时延定时器
TUP T12	15	(范围：4~15 sec 默认：15)	等待闭塞证实信号定时器
TUP T15	15	(范围：4~15 sec 默认：15)	等待解除闭塞证实定时器
TUP T18	15	(范围：4~15 sec 默认：15)	等待电路复原信号响应定时器
TUP T21	15	(范围：4~15 sec 默认：15)	等待电路群复原证实消息定时器
TUP T26	15	(范围：4~15 sec 默认：15)	等待面向维护的群闭塞证实消息定时器
TUP T28	15	(范围：4~15 sec 默认：15)	等待面向维护的群闭塞解除证实消息定时器

刷新 提交

Figure 1-112 TUP timer configuration

The above timer is mainly used for the signaling exchanging when binding the ISUP or TUP protocol. The main timers and the functions are as follows:

MTP2 T1 timer	Locating ready timer
MTP2 T2 timer	Un-located timer
MTP2 T3 timer	Located timer
MTP2 T4 timer	Normal checking and accepting period timer
MTP2 T5 timer	Send SIB timer
MTP2 T6 timer	Remote block timer
MTP2 T7 timer	The verification delay timer controlled by the error
MTP3 T1 timer	The delay of avoiding the order error after message changeover
MTP3 T10 timer	Waiting for re-transmitting signal route group test message
MTP3 T11 timer	Limited transmission timer
MTP3 T12 timer	Waiting for removing the block verification
MTP3 T13 timer	Waiting for forced removing block
MTP3 T14 timer	Waiting for the block verification
MTP3 T15 timer	Waiting for enabling the signaling route group block test
MTP3 T16 timer	Waiting for modifying the route group block status
MTP3 T17 timer	The delay of avoiding the initial locating fault and link re-starting
MTP3 T2 timer	Waiting for the changeover verification
MTP3 T22 timer	Local block test timer
MTP3 T23 timer	Remote block test timer
MTP3 T3 timer	Time controlled transmission-delay of avoiding order error after changeover
MTP3 T4 timer	Waiting for the changeover verification (first try)
MTP3 T5 timer	Waiting for the changeover verification (second try)
MTP3 T6 timer	Message order error delay after avoiding controlled re-selected route
MTP3 T7 timer	Waiting for the signaling data link connection verification
MTP3 T8 timer	The suppression timer of prohibiting transmission
TUP T1 timer	The timer of waiting for the connection or connection failure signal
TUP T10 timer	The delay timer of repeated continuity checks
TUP T12 timer	The timer of waiting for the block verification signal
TUP T15 timer	The timer of waiting for removing the block verification
TUP T18 timer	The timer of waiting for the circuit restoration signal response
TUP T2 timer	The timer of waiting for the address full message
TUP T21 timer	The timer of waiting for the circuit group restoration verification message
TUP T26 timer	The timer of waiting for the maintenance-oriented group block verification message
TUP T28 timer	The timer of waiting for the maintenance-oriented group block removing verification message
TUP T3 timer	The timer of waiting for the clear forward signal after

	sending the failure message
TUP T4 timer	The timer of waiting for the clear forward signal after sending the call failure signal
TUP T6 timer	The timer of waiting for releasing guarding signal
TUP T9 timer	The timer of enabling the first continuity-check verification

Operation Status Monitoring

Operation Status Monitoring

The interface is used to display the CPU information, memory information and fan information (only 6500 has the information) in the device. Click **CPU Information** or **MEMROY Information** or **Fan Information** to switch over the CPU information, MEMORY information and fan information, as follows:

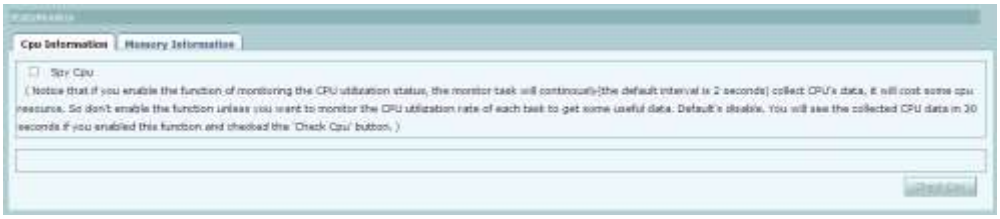


Figure 1-113 CPU information

Caution

The above figure is the CPU information of MyPower VGA600, VG800, VG2000, and VGM6000.

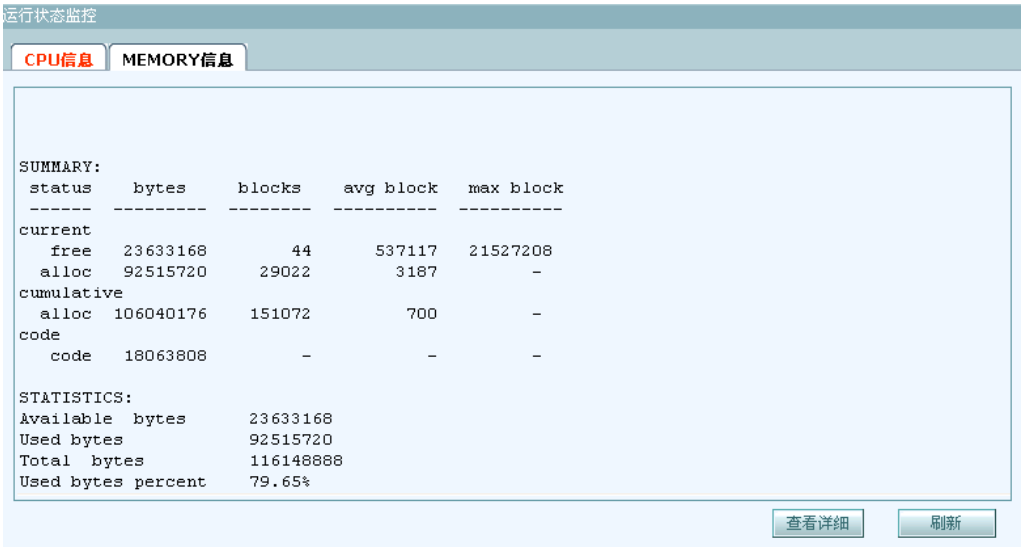


Figure 1-114 MEMORY information

Caution

The above figure shows the memory information of MyPower VGA600, VG800, VG2000, and VGM6000.

CPU information: Click **CPU Information** to display the CPU information, as follows:

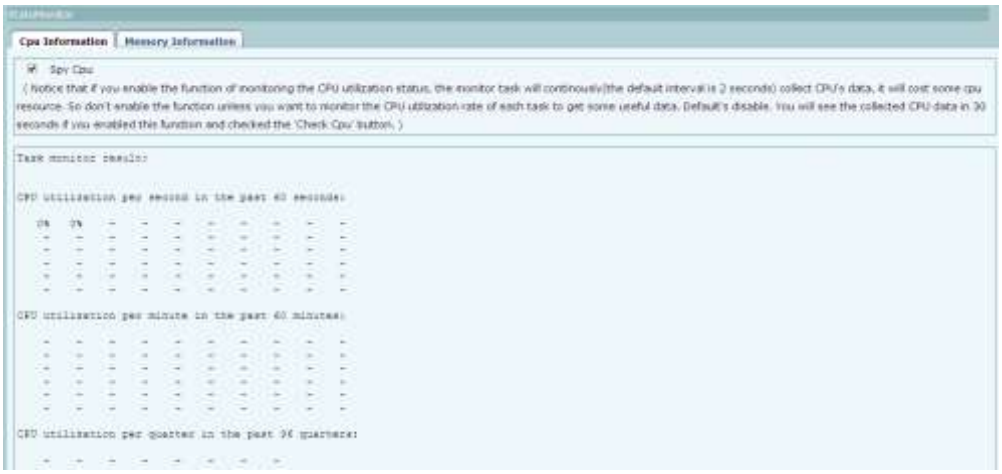

Cpu Information
Memory Information
Spy Cpu
Task monitor result:
CPU utilization per second in the past 60 seconds:
CPU utilization per minute in the past 60 minutes:
CPU utilization per quarter in the past 24 quarters:

Figure 1-115 CPU information

MEMORY information: Click **Check Detail**, as follows:

Figure 1-116 MEMORY information

Route Configuration

Supporting Devices

MyPower VGA600, MyPower VG2000, MyPower VG800, MyPower VGM6000, MyPower VGM 6500

Static Route Configuration

The static route is the customized route, which makes the transmission of the IP packets between the source and destination adopt the specified path. This section describes how to configure the static route on the voice gateway for the network interconnection.

Enter the configuration interface and you can see the configured static route information. Click ✕ to delete the route information. To add one static route information, input the correct destination address, destination address subnet mask and gateway address, and then click **Apply**.

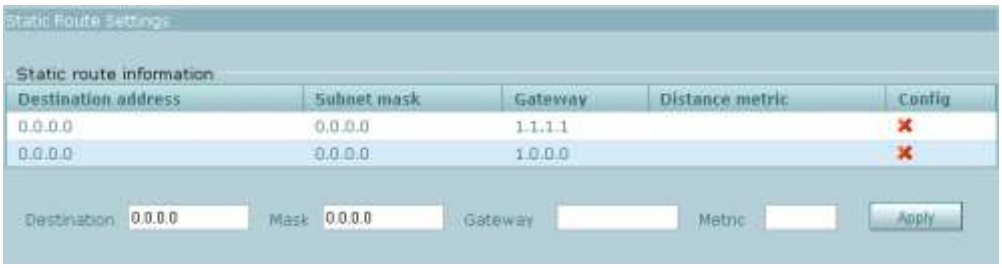


Figure 1-117 Static route configuration

Destination: The address of the remote network; for example, for class-C address, the network address is the front three fields and the last field is 0;

Mask: The subnet mask of the destination address; if the destination address is class-C address, the mask should be 255.255.255.0;

Gateway: The data delivering gateway address matching with the destination network;

Metric: The metric value; the number of the route nodes to the destination address;

System Management

Supporting Devices

MyPower VG2000, MyPower VG800, MyPower VGA600, MyPower VGM6000, MyPower VGM6500

Basic Information Configuration

The basic information configuration is the configuration and display of some basic information, such as system name, system time, contact name, telephone number, physical location and the normal running time of the system.

Enter the configuration interface and you can see the configured basic information.

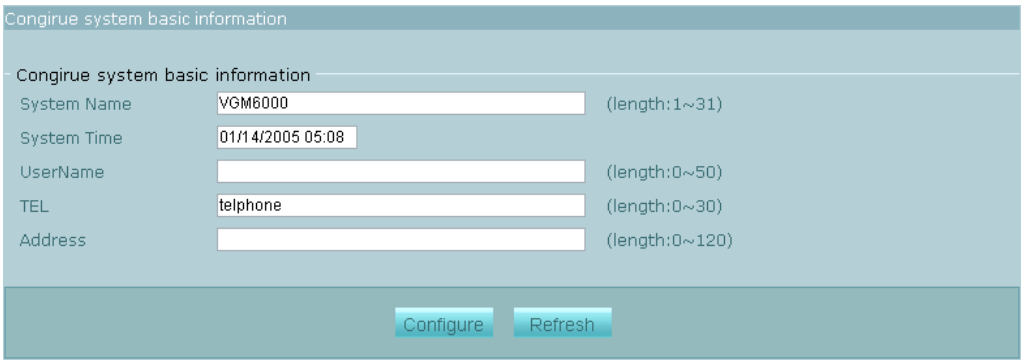


Figure 1-118 Basic information

System Name: The name of the voice gateway; if the item setting is changed, it takes effect at once and do not need to restart the system;

System Time: The system clock time of the voice gateway;

UserName: The name of the contact;

TEL: The telephone number of the contact;

Address: The address of the contact;

System Running Normally: The normal running time of the voice gateway since power on.

Administrator Setting

The voice gateway can set different levels of users, such as the administrator user **admin** and common user **guest**. The administrator has the largest authority and can modify the passwords of himself, guest and other customized user, set the enable password, and enable or disable the guest user. If logging with the guest user, the interface only displays the guest user, but does not display the admin user. The guest user can his password only on the interface and cannot view the contents of the voice configuration. After modifying and setting successfully, the web interface prompts to input new password at once. After inputting the new password, the user can browse or configure other interfaces.

Figure 1-119 Administrator setting

Device Software Upgrade

Upgrade Program via WEB

You can upgrade the web management system and device IOS program on the interface.

Figure 1-120 Device software upgrade

After upgrading the web management system, WEB prompts the user whether to delete the old web program. After clicking **Yes**, delete the old WEB management system program and apply the new WEB management system program. If the user clicks **Cancel**, the old WEB management system program is not deleted, but directly apply new WEB management system program. It is recommended to click **Yes** to delete the old management system program, avoiding that the system flash is not enough.

Upgrade the application program of the IOS device. You can upgrade and update the application program of the IOS device via WEB. The extension name of the application program file of the IOS device is .bin (such as VPM600-VG-8.0.41.bin). Ensure that the IOS program to be upgraded matches with the device. After upgrading the application program of the IOS device, you need to restart the device.

When using the web management system to upgrade the program, the system may prompts the following dialog box:

Windows Internet Explorer
Failed to update the web program!
Maybe there are too many old web programs make the memory insufficient. Delete all the old web programs could resolve this problem.
Notice: If restart the device without updating the WEB to new WEB program after you removed all the old WEB program, the WEB might be unusable after reboot.
Are you sure to delete all old web programs?
确定
取消

Figure 1-121 Upgrading WEB fails

The dialog box prompts that upgrading the user program fails. The failure reason may be that the device FLASH or memory space is not enough. If FLASH is not enough (if not sure, you'd better log into the device via Telnet to view whether the remaining FLASH space is enough to hold the files). You can click **Yes** to delete the old program in FLASH to solve the problem. Otherwise, maybe it is caused by the unexpected abnormal problem during the file upgrade. It is recommended not to delete the old program, but search for the problem reason and solution.

Besides, you can restart the device on the interface. To restart the device, click **Restart Device**. When the user is sure to restart the device, WEB prompts the user whether to save the current configuration. To ensure that the configuration after restarting the device is consistent with the current configuration, it is recommended to save the current device configuration.

Caution

1. After upgrading the web management system, the browser may use the buffered old interface file. Please clear up the buffer of the IE browser and access again, so as to ensure that the accessed is the latest interface.

2. The IOS file is the application program of the device.

3. When using the upgrade program of the web management system, the directory of saving the file to be upgraded cannot be too long. It had better be saved in the root directory. If the file directory is too long, uploading the file may fail.

Configuration File Management

You can back up or restore the configuration file of the device on the interface. Click **Backup**, select the path of saving the backup file, click **Yes** and you can download the configuration file of the current gateway to the PC hard disk of the administrator. If you want to use the existing configuration file to cover the configuration on the current gateway, click **Browse**, select the desired configuration file and click **Recover**. After the operation succeeds, the system prompts whether to restart the device, because the new configuration can take effect only after restarting the device. Therefore, it is recommended to select **Restart**.

The configuration file management includes:

Back up the system configuration file:

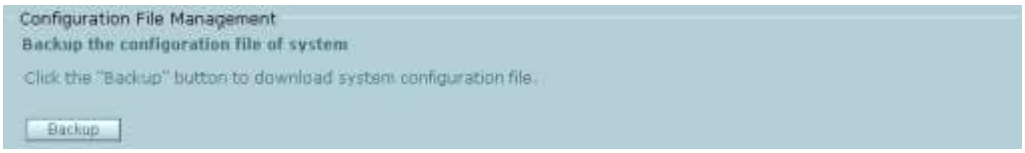

Configuration File Management
Backup the configuration file of system
Click the "Backup" button to download system configuration file.
Backup

Figure 1-122 Configuration file management

Click **Backup** to download the configuration file of the device to the local.

Restore the system configuration file:

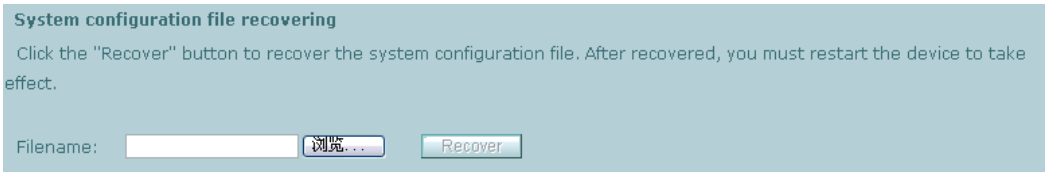

System configuration file recovering
Click the "Recover" button to recover the system configuration file. After recovered, you must restart the device to take effect.
Filename:
浏览...
Recover

Figure 1-123 Configuration file management

To recover to the previous configuration, find the configuration file at the local and then click **Recover**.

Log Management

Display the log information saved in the flash.

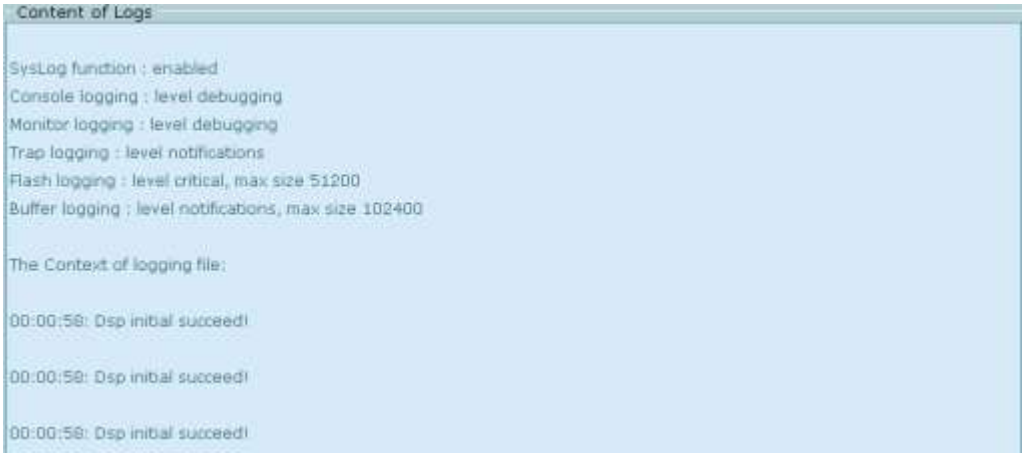

Content of Logs
SysLog function : enabled
Console logging : level debugging
Monitor logging : level debugging
Trap logging : level notifications
Flash logging : level critical, max size 51200
Buffer logging : level notifications, max size 102400
The Context of logging file:
00:00:58: Dsp initial succeed!
00:00:58: Dsp initial succeed!
00:00:58: Dsp initial succeed!

Figure 1-124 Log management

Figure 1-125 Log management

Define log message level

Level	Description
0	The system is unavailable
1	Need to take action at once
2	The crisis state
3	The error state
4	The alarming state
5	The normal, but notable state
6	Just the report message
7	Debug information

The content similar to the following is displayed in the log.

%SYS-5-LOGIN:

Here, 5 in "%SYS-5-LOGIN" indicates the level and you can find its description the above table.

Caution

Click Clear to prompt whether to clear up all logs. If selecting **Yes**, clear up all logs, so be careful.

SNMP Parameter Configuration

SNMP (Simple Network Management Protocol) is one standard protocol of managing Internet. The purpose is to ensure that the management information can be transmitted between Network Managing Station and the managed device-Agent. It is convenient for the system administrator to manage the network system. For the details of the SNMP protocol, refer to the materials about the TCP/IP protocol.

Enter the **Configuration of SNMP parameters** interface via Navigation Bar->System Management->Configuration of SNMP parameter, as follows:

Figure 1-126 SNMP parameter configuration

Start the SNMP Agent: Tick the check box and the network management agent process is enabled on the voice gateway. The network management software can manage the voice gateway via SNMP.

Community name table contains two configuration items, that is, community name and operation authority. The community name specifies the community to which the voice gateway is added. The community name should be the same as the community name configured on the network

managing station. Otherwise, the network managing station cannot perform any operation for the voice gateway. The operation authority specifies the operation authority of the SNMP management station corresponding to the community name for the managed devices, including read-write and read only.

TRAP host name table includes the host name and community name. The host name can be configured as the host name or IP address of the SNMP trap packet sent by the receiving device. Usually, it is the address of the network management station. The community name is the community to which the management station for receiving the TRAP packets belongs. It can be the same as or different from the community name in the SNMP community name table.

Click and and you can edit and delete the corresponding item. Click **Add community** and **Add TRAP Host**, and you can add the items of the SNMP community name table and TRAP host name table.

The community name, operation authority and the host IP address of receiving traps packets can be set only when the SNMP agent is enabled, so the parameters cannot be set when the gateway does not enable the SNMP agent.

📖 **Note**

Currently, the WEB interface only supports the SNMPv2 configuration. To configure the SNMPv1 or SNMPv3 parameters, as well as the other parameters of SNMPv2, log into the device via Telnet or Console port and configure via the shell interface.

TRAP receiving host can be configured as the host name or IP address. When being configured as the host name, confirm whether you have configured the mapping of the host name and IP address in the host name and IP address mapping tables of the device. The mapping of the host name and IP address needs to be configured via shell.

Save Configuration

The function of the chapter is to save the current setting on the device.

The user can save the current configuration as the configuration parameter for starting the switch next time after modifying the system configuration and passing verification.

Click

of the navigation bar and the system prompts the dialog box. Select **Yes** to save the current configuration and select **Cancel** to cancel the saving operation.

Typical Applications

In this chapter, we aim to assist the user to perform basic application configuration of the VGA600 gateway via a typical application example of VGA600 gateway, including local FXS port, FXO port configuration, H323 configuration, fax configuration, communications between locals, between local and H323, between local and PSTN, and realization of fax function.

Environment

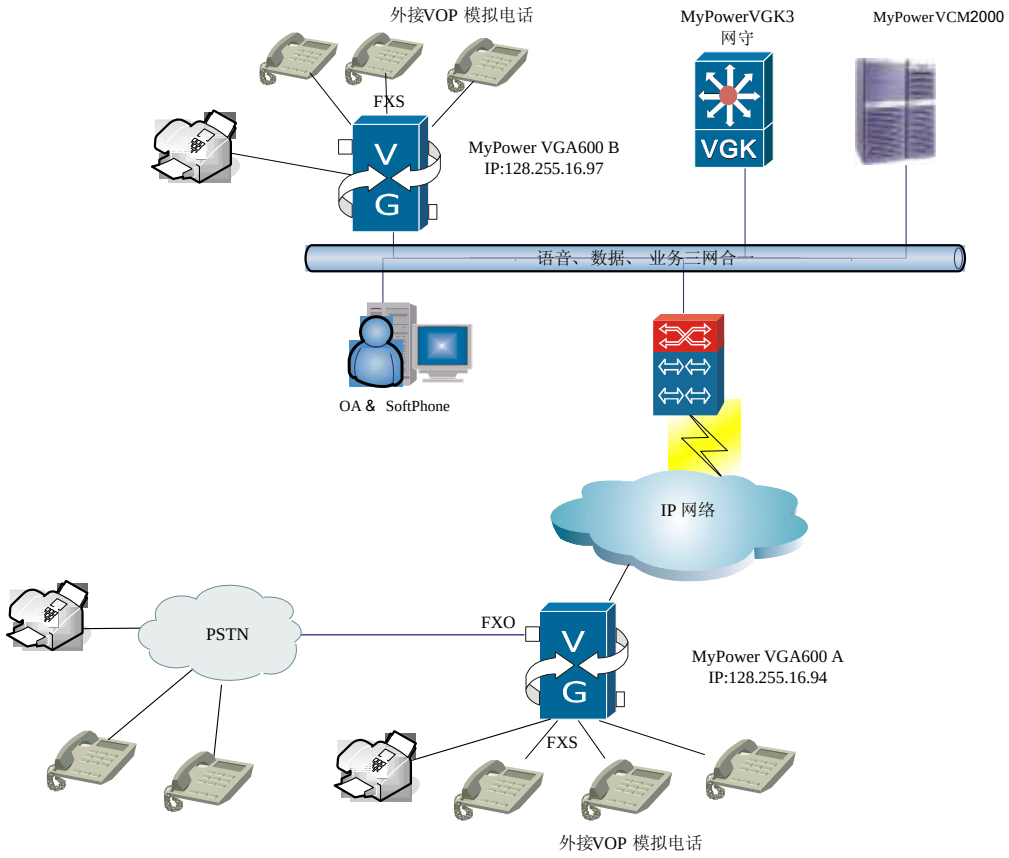


Figure 2-1 Environment description

The figure above shows a typical voice application of the VGA600 gateway. VGA600 gateway connects to another Ethernet via IP network, so as to perform communication and faxing with IP phones in other Ethernets. At the same time, VGA600 gateway can realize communication and faxing

with traditional phones by accessing PSTN traditional telecom telephone network via FXO port. In such case, VGA600 gateway equals to a small PBX.

Configuration Steps

Let's start now to configure one VGA600 gateway or several VGA600 gateways owned by you. It is easy to perform configuration since VGA600 gateway provides you with very friendly WEB configuration interface and many helps.

Communication Configuration between Local and H323

After getting the VGA600 gateway, you need to configure the communication between the local FXS and other gateway or IP phone on the IP network manually. Suppose that the local voice gateway is VGA600 A and the remote voice gateway is VGA600 B. Now, we configure the H323 communication between the FXS port of VGA600 A and the FXS port of remote IP phone VGA600 B via the IP network, as shown in the above figure.

WAN Configuration

To realize communication with IP phone of H323 side, we must allocate a WAN IP address for VGA600 gateway that we use. The following takes VGA600 A as an example. The steps are as follows:

Enter **WAN configuration**-> **Configuration Wizard of Accessing WAN** from navigation bar and then configure WAN accessing step by step according to wizard. First, enter the interface as follows:

Configuration Wizard of Accessing WAN
This wizard will lead you to connect your device to Internet step by step.
Step 1 : Choose the interface to be configured.
Step 2 : Choose the type that you use to connect to the WAN.
Step 3 : Configure other options, basing on the type you have chosen in the Step 2.
Next
Exit

Figure 2-2 Access configuration wizard

Click **Next** to enter the **Choosing Interface for WAN Connection** interface, as follows:

Configuration Wizard of Accessing WAN - Choosing Interface for WAN Connection
The router can connect to Internet via multi-interface. Please choose the corresponding interface according to the cable or fibre that you used.
Choose the interface
WAN
Previous
Next
Exit

Figure 2-3 WAN connection interface

Choose the port fastethernet0 and then click **Next** to enter the **WAN Connection Type** interface, as follows:

Figure 2-4 WAN access type

The WAN port of the VGA600 gateway has three kinds of line connection modes, as shown in the above figure. The application example takes **Fixed Address Line** as an example. Select **Fixed Address Line**, click **Next** and the following interface is displayed.

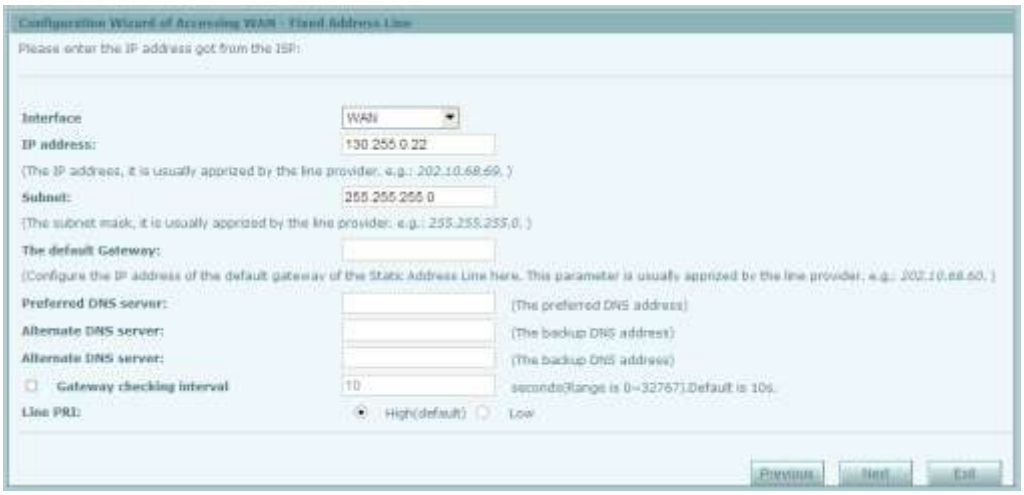

Configuration Wizard of Accessing WAN - Fixed Address Line
Please enter the IP address got from the ISP.
Interface
WAN
IP address:
130.255.0.22
(The IP address, it is usually apprized by the line provider, e.g.: 202.10.68.69.)
Subnet:
255.255.255.0
(The subnet mask, it is usually apprized by the line provider, e.g.: 255.255.255.0.)
The default Gateway:
(Configure the IP address of the default gateway of the Static Address Line here. This parameter is usually apprized by the line provider, e.g.: 202.10.68.60.)
Preferred DNS server:
(The preferred DNS address)
Alternate DNS server:
(The backup DNS address)
Alternate DNS server:
(The backup DNS address)
Gateway checking interval
10
seconds(Range is 0~32767,Default is 10s.
Line PRI:
High(default)
Low
Previous
Next
Exit

Figure 2-5 Fixed address line

In the above figure, set the WAN IP address of VGA600 A gateway as 130.255.0.40, and subnet mask as 255.255.252.0.

WAN port configuration has been completed here. You can click **WAN Configuration**->**WAN port Connection information** to view all WAN configuration information, as follows:

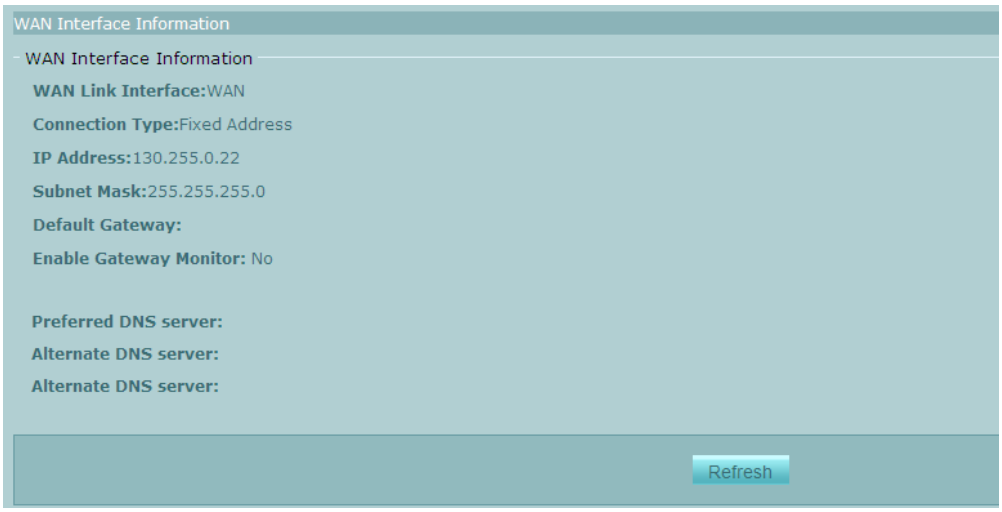


Figure 2-6 WAN connection information

Protocol Configuration

In the last step, we have performed WAN configuration for the gateway, but it is impossible to realize WAN communication only based on it. MyPower VG VoIP gateway supports H323 protocol and SIP protocol. Now, we take H323 protocol as the example to configure protocol for remote IP phone communication. Take VGA600 A as an example to describe.

Enter **Voice Configuration**->**Protocol Configuration** in navigation bar, as follows:

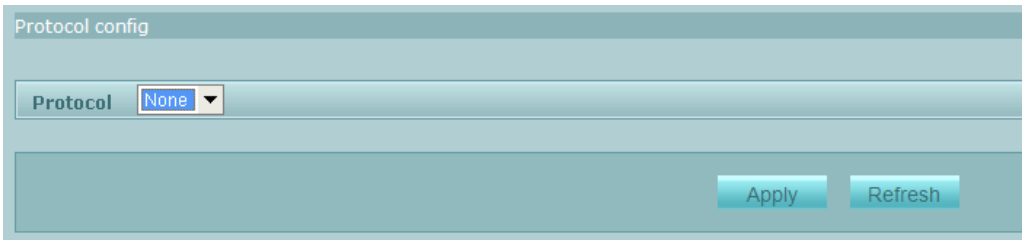


Figure 2-7 Protocol configuration

Choose a desired protocol from the drop-down box. There are three options, that is, none, H323 and SIP. In this example, we choose H323 protocol. The following figure shows configuration given by the system after choosing H323 protocol:

Figure 2-8 H323 protocol

If there is a gatekeeper in the network, fill in the address of the gatekeeper and then register to the gatekeeper. Click **Apply** to save the configuration information. If the system prompts the setting success, it indicates that the setting of the gateway registration succeeds. Otherwise, the setting fails. Enable **Register to gatekeeper** and you can view whether the current registration succeeds.

Use the same method to set the current running protocol of VGA600 B as the Ha323 protocol, so as to ensure that gateway A and B can communicate with each other normally.

Now, we still cannot communicate with IP phones of other gateways on the IP network. We don't know whom we communicate with and how to communicate. In next section, we will perform call route configuration, so as to complete communication between local FXS and IP phones of other gateways in IP network.

Configure Call Route

Click **Voice Configuration->Call Route Configuration** in WEB Navigation Bar of VGA600 A to enter the following interface:

Figure 2-9 Call route configuration

Click **Add** in **VOIP Configuration** and **POTS Configuration** to configure the call route of VGA600 A gateway. VOIP dialer configures the call route of the communication over the IP network to correspond to VGA600 B. POTS dialer configures the route of the local number to correspond with the ports of the local gateway.

Click **POTS Configuration** to enter the POTS dialer (local number) configuration interface and then click 'Add' to enter the following interface:

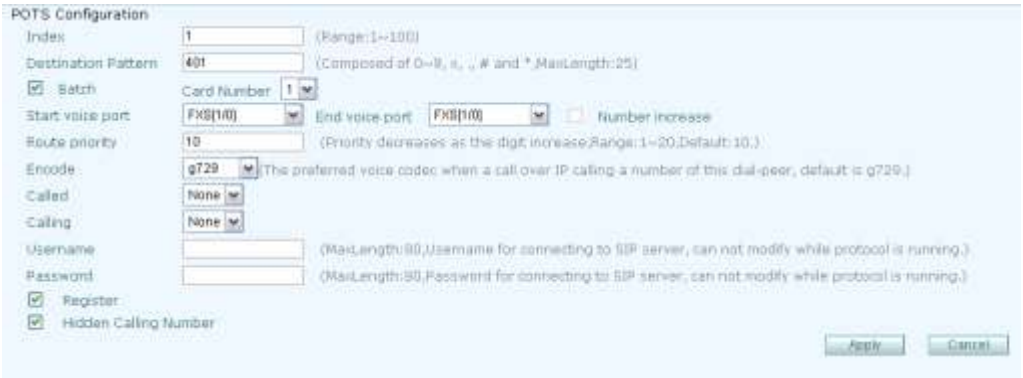


Figure 2-10 Add POTS configuration

In the above figure, configure one batch POTS route, the start voice port is FXS[0/0] and the end port is FXS[0/2]. The start number is 234, which increases by 1 according to the port serial number, that is, ports FXS[0/0]~FXS[0/2]3 correspond with the telephone number 234 to 236.

Click **Apply**. If the system prompts success, you can see the following information in **POTS Configuration** of **Voice Configuration** -> **Call route configuration**:

Figure 2-11 POTS configuration

In this way, the telephone number of the local FXS port of VGA600 A is configured. Next, we need to configure the VoIP route of the peer VGA600 B.

Select **VoIP Configuration** in the above figure, and click **Add** to enter the following interface:

Figure 2-12 VOIP configuration

In the above figure, the VoIP call route with the serial number 4 is configured. The route target is VGA600 B. One local telephone number 2008 is configured on VGA600 B (the configuration method is the same as the above method). When configuring the telephone number on the peer gateway, we can use x to match. For example, configure 16 telephone numbers 2000~2015 on VGA600 B. If we want to configure the route matching the 16 numbers on VGA600 A, we can perform the following configuration:

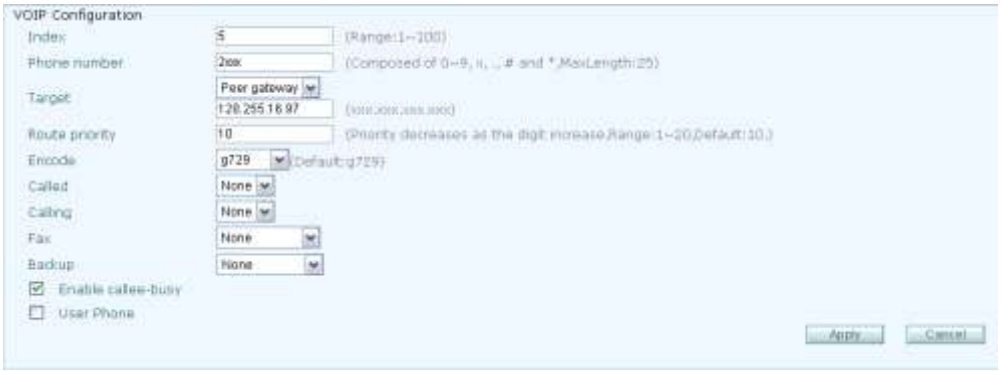


Figure 2-13 Add VOIP configuration

2xxx in the above figure can match all telephone numbers beginning with 2 and with the length as 4 on VGA600 B.

Click **Apply** to configure the call route information. In **Voice Configuration** -> **Call route configuration**, you can see all configured call route information, as follows:

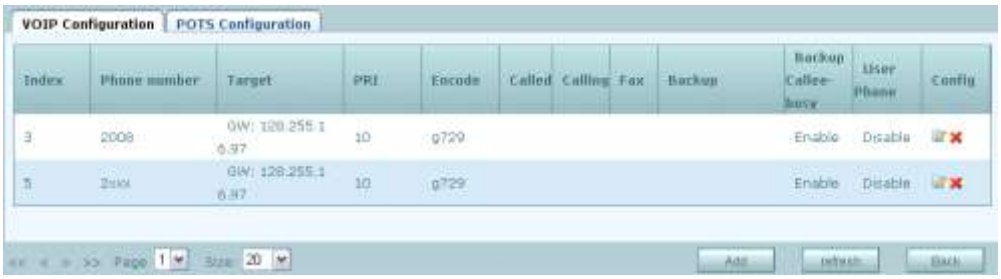


Figure 2-14 VOIP configuration

Up to now, the basic configuration of the communication between the local FXS port and H323 side is complete. Now, pick up the phone and dial the configured peer telephone number.

Communication Configuration between FXS and PSTN

We can communicate with the telephone on PSTN via the FXO port. Take VGA600 A as an example. When the FXO port is connected to PSTN, VGA600 A is regarded as one special phone on the PSTN phone network. The other PSTN phone can communicate with the other IP phones on VGA600 by dialing the PSTN telephone number of the FXO port of VGA600 A. Similarly, the IP phone on VGA600 A can dial any phone on PSTN via the FXO port. In this section, we configure the communication between FXS and PSTN.

Enter **Voice Configuration** -> **Voice port configuration** in the navigation bar, as follows:

Figure 2-15 Voice port configuration

Tick the check box at the left of the FXO port and then click **Advanced Configure** to enter the following interface:

Figure 2-16 Advanced configuration of FXO port

Invert the **Disable** check box to enable FXO port. Pay attention to the **Connection-plar** option on the interface. It refers to the corresponding telephone number or FXS port of VGA600 A when PNST is dialing FXO port.

Select FXS port and a drop-down list with all FXS ports of the current gateway is displayed. You can select the desired FXS port which the FXO port needs to be bound with from the drop-down list. When PSTN dials the telephone number of the FXO port, the gateway automatically searches the configured telephone number of the FXS port bound with the FXO port and initiates a call.

If configured as number, there are three kinds of filling modes:

It can be configured as any complete number of FXS port on VGA600 A, such as 2008.

It also can be the business number of some business configured by VGA600 A. Take IVR secondary dialing access number as an example. On the premise of IVR access number, if the user dials exterior line number of FXO by PSTN phone, it is transferred to the gateway IVR voice interactive system directly.

Or the user can leave it blank. When PSTN user dials FXO port, he hears the long ring-back tone that reminds you of dialing extension of VGA600 A.

Fill the blank with a connection-plar type and save it.

Call route Configuration

Click **Voice Configuration**->**Call Route Configuration** in the navigation bar to enter the interface displayed below. Choose port FXO[0/3] from the

Voice Port drop-down list. We configure FXO here as trunk interface to connect with telecom PSTN network. Then the user can dial original exterior line number via VGA600 A. See the configuration in the following figure:

Figure 2-17 POTS configuration

Click **Apply**. In the following figure, we can see that the call route 5 of one number matching rule "xx." (it can match any legal number) is configured for port FXO[0/3]. As a result, VGA600 A can call the other number in PSTN via the dialer.

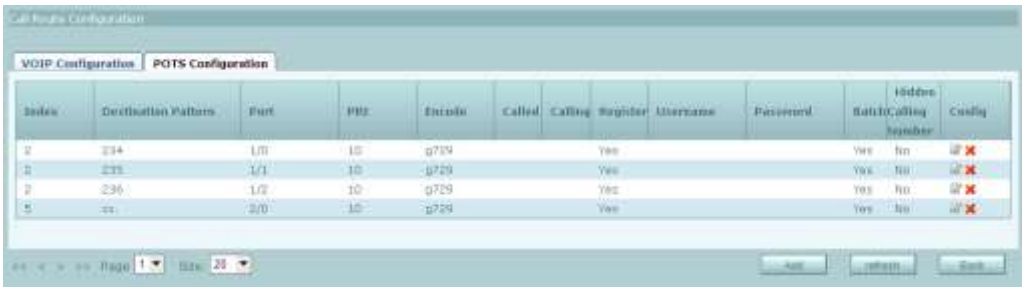


Figure 2-18 POTS configuration

Now, we have completed the configuration for the communication between FXS and PSTN. Let's dial a PSTN number by IP phone.

Number Transform Configuration for PSTN Port:

For programming dialing type conveniently, we need to identify numbers of different types. For example, PSTN numbers start with 028 and IP numbers start with 193. In such case, it is easy for us to identify PSTN number and IP number.

We have described in detail the configuration of number transform in section 1.4.4, so we skip it here. The figure below shows a number transform rule with index as 1. The rule of this index is to delete prefix 028 from the numbers beginning with 028.

Figure 2-19 Number transform configuration

If just configuring the number transform rule on the gateway, but not applying it on one dialer, the rule does not take effect. That is to say, the number transform rule can take effect only after being bound with the dialer, as follows:

Figure 2-20 POTS configuration

In the above figure, we configure the telephone number of FXO[0/3] at POTS dialer as 0286xxx and select the rule with index as 1 in the transform rule of called number. Thus, when the user dials numbers beginning with 028, device will delete 028 first and then seek for call route according to number match rule. For example, when calling number 028601 in VGA600 A dials 0286004, the called number will be transformed into 6004 according to number transform rule, so as to accord with one number in PSTN.

IP Fax Configuration

Fax is a common telephone business we use in daily work. Enter fax service configuration page by clicking **Voice Configuration**->**Fax Service Configuration** in navigation bar:

Figure 2-21 Fax service configuration

There are two fax modes for MyPower VG VoIP gateway, that is, T32 fax mode and transparent transmission mode. We will perform configurations here for these two fax modes. Take VGA600 A as an example.

In the figure above, tick the **Enable the global T.38 capability of this gateway** checkbox to make all gateways support T38 fax capability. Or the user can enable T38 capability under some dial-peer only or disable T38 capability under some dial-peer, or enable transparent transmission mode according to requirement. In such case, **Enable the global T.38 capability of this gateway** means to check fax capability and its type according to the specific settings of each dial-peer. Enter **Voice Configuration**->**Call Route Configuration**, as follows:

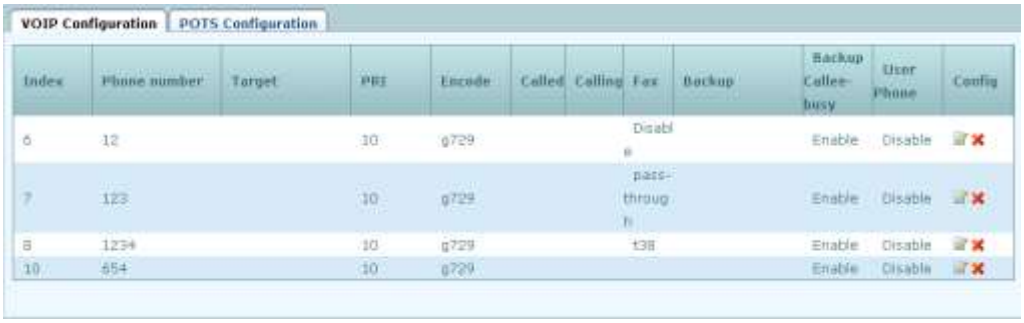


Figure 2-22 VOIP configuration

In the above figure, the fax capability of Index 8 is t38. The fax protocol of Index 9 is pass-through, that is, fax transparent transmission mode. The fax protocol of Index 10 is not configured. If the user configures "**Enable the global T.38 capability of this gateway**", the port will fax in T38 fax mode. Otherwise, it has no fax capability. How to configure fax capability of each dial-peer? You must keep a point in your mind: only under VOIP dial-peer.

Click the icon at the right of Index 5 to enter the following interface:

Figure 2-23 VOIP dialer configuration

In the above figure, you can see that the system provides four options in the drop-down list at the right of the Fax option. The first option is "-", which is the default value of the VoIP dialer. "Disable" indicates that the fax capability of this dial-peer is disabled. If selecting T.38, adopt T38 protocol to fax. If selecting pass-through, adopt the transparent transmission mode to fax and it is required that the code types of the two gateways should be consistent. For example, if we set it as G729, the peer gateway of the fax should also be G729.

If the user does not configure "**Enable the global T.38 capability of this gateway**", but the T.38 fax is configured in the dialer, carry the T38 capability when the gateway serves as the caller; backward learn the call route table to determine whether to support the T38 fax according to the caller number when the gateway serves as the callee.

For the explanation of the other configuration items, refer to the section of Fax Service Configuration.

Note

When the gateway serves as the called to receive IP calls, it first queries the dialer of the calling number to determine its own fax type. For example, if the 654 in the above configuration calls in, the fax capability of the gateway is confirmed as transparent transmission; if 2010 calls in, the fax capability of the gateway is confirmed as T38. If 234324 calls in, the fax protocol of Index 10 is not configured, so adopt the global fax capability. If the local fax mode is confirmed, it is required that the peer party should be configured with the desired fax mode so that the fax can be performed normally.